Ministerie van Economische Zaken

Security First

Een verkenning naar Nederlandse kansen voor veiligheid en innovatie

Colofon

Onderzoek
Dit onderzoek is uitgevoerd door:
SenterNovem, Innovation Intelligence & Coordination, in samenwerking met de ministeries van Economische Zaken, Defensie, Binnenlandse Zaken & Koninkrijksrelaties en Justitie.

Contactpersoon
Voor meer informatie kunt u contact opnemen met:
Dr. M.J. (Marcel) Kleijn
Tel.: +31 (0)70 3735324
E-mail: m.kleijn@senternovem.nl

Rapport informatie
Datum: 19 november 2007
Kenmerk: DII0790477
Status: Definitief

Projectgroep
De auteurs zijn:
Hin Oey, Chantal Wentink, Arjen Goetheer, Marcel Kleijn
De begeleidingsgroep bestaat uit de volgende leden:
Astrid Boschker (EZ), Margo Strijbosch (EZ), Roel van Pelt (EZ), Dimitri van Rijn (Defensie), Rob Dekker (Defensie), Peter Niessen (BZK), Michiel van der Duin (BZK), Bram Foederer (Justitie)

Met dank aan
TNO, NIID, TU Delft, Octrooicentrum Nederland, Informatiecentrum EZ, TWA Netwerk, Syntens, Technopartner en vele anderen

INNOVATION INTELLIGENCE

Security First - een verkenning naar Nederlandse kansen voor veiligheid en innovatie

Inhoudsopgave

Samenvatting

Achtergrond

Veiligheid is één van de basisbehoeften van de samenleving. Technologie en innovatie als zodanig bieden niet dé oplossing voor veiligheidsvraagstukken, maar oplossingen zonder technologie en innovatie zijn nauwelijks denkbaar. Ze zijn dus van groot belang voor veiligheid. Nederland zet de komende jaren sterk in op innovatie en veiligheid, via pijler 2 van het Beleidsprogramma van het kabinet Balkenende IV. Daarin wordt onder meer de ambitie neergelegd om een maatschappelijke innovatieagenda voor Veiligheid op te stellen. Deze verkenning vormt input voor het opstellen van deze agenda.

Afbakening

Deze verkenning gaat uit van Veiligheid in de zin van 'security' en niet van 'safety'. Het begrip veiligheid zoals dat in deze verkenning wordt gehanteerd omvat vraagstukken en/of toepassingen als: preventie, bescherming en optreden tegen criminaliteit en overlast, crisisbeheersing, rampenbestrijding, gecoördineerd optreden van veiligheidsdiensten, brandveiligheid, persoonlijke veiligheid van veiligheidspersoneel, terrorismebestrijding en radicalisering. Thema's als externe veiligheid, beveiliging tegen watersnood en vliegveiligheid vallen daarmee niet binnen de scope van deze verkenning. De beheersing van crises en rampen die het gevolg zijn van milieurampen, overstromingen en vliegrampen, vallen echter wel binnen de scope van deze verkenning. Als uitgangspunt voor het aanbod van oplossingen is verder genomen dat het moet gaan om innovatieve oplossingen die toepasbaar zijn voor zowel civiele/maatschappelijke/sociale veiligheid als externe veiligheid (Defensie).

De veiligheidssector in beeld

Verschillende actoren zijn relevant als het gaat om Veiligheid. Allereerst de overheid, vanuit haar rol als vragende partij. Het betreft hier de centrale overheid: de ministeries van BZK, Justitie, Defensie, VWS, VROM, V&W en EZ en hun diensten zoals de politie, het Nationaal Coördinatiecentrum (NCC), de Nationaal Coördinator Terrorismebestrijding (NCTb) van BZK en de Douane van Financiën. De provincies en gemeenten behoren ook tot deze actor. De overheid is een belangrijke speler en heeft op bepaalde onderdelen een monopoliepositie zoals defensie en politie. Het is aan de overheid de samenleving enerzijds te behoeden voor grootschalige incidenten, crises en rampen, maar anderzijds ook de samenleving hierop voor te bereiden. De overheid articuleert haar vraag naar oplossingen onder meer via de arena's Maatschappelijke Veiligheid en Defensie.

De kennisinstellingen en universiteiten spelen ook een belangrijke rol, omdat zij voornamelijk de kennisbasis verzorgen voor de technologische en innovatieve oplossingen. TNO Defensie en Veiligheid is hier bijvoorbeeld een zeer belangrijke speler. Bedrijven zorgen vervolgens voor de implementatie van deze oplossingen en de toepassing naar Veiligheid. Bedrijven zijn daarnaast ook een vragende partij. Er zijn naar schatting ruim vijfhonderd bedrijven in Nederland actief op het terrein van Veiligheid. Zowel grote spelers (Philips, Thales) als vele kleinere, waaronder starters en spin-offs van universiteiten en kennisinstellingen.

Karakteristieken van veiligheid en innovatie

Het veiligheidsveld onderscheidt zich op verschillende punten van andere domeinen. Bij het opstellen van een toekomstig innovatieprogramma zijn de specifieke karakteristieken van het veiligheidsveld bepalend voor de meest effectieve (stimulerings)maatregelen en activiteiten die worden ondernomen. De karakteristieken worden hieronder kort samengevat.

- *De overheid is een grote speler en belangrijk als eerste klant*
  Voor politie, defensie en veiligheidsdiensten heeft de centrale overheid een monopolistische rol. Voor een ander deel heeft de centrale overheid vooral een faciliterende rol, zoals bij de brandweer. Bij grootschalige incidenten, crises of rampen, heeft de centrale overheid een coördinerende rol. Door het maatschappelijke belang van veiligheid is de Nederlandse overheid vaak de belangrijkste klant is voor een nieuw product of dienst. De overheid kan als 'launching customer' dus een belangrijke rol spelen bij het sneller ontwikkelen en toepassen van innovatieve oplossingen.

- *Er is een trend van 'made to measure' naar 'commercial of the shelf' (COTS)*
  Recent was er veelvuldig sprake van 'made to measure'. De overheid (met name Defensie) was nauw betrokken bij de vraagformulering en het ontwikkelingstraject en was ook 'bij afspraak' koper van de operationele oplossingen. Het bedrijfsleven was zeker van de overheid als klant. Er is nu meer sprake van een situatie waarbij de overheid niet meer automatisch garant staat voor aanschaf. Men wil kunnen kiezen uit oplossingen die commercieel beschikbaar zijn. Een tweede ontwikkeling is dat specifieke overheidsopdrachten onvoldoende zijn voor bedrijven om productie te rechtvaardigen. Dit impliceert dat de toepassing van innovatieve oplossingen niet alleen met de overheid als klant gerealiseerd kunnen worden.

- *Er is een wereldmarkt, maar grote landen hebben nog afgeschermde markten*
  In elk land is er een markt voor Veiligheid. Echter, in de landen met een omvangrijke nationale defensie-industrie kijkt de overheid over het algemeen eerst naar de nationale industrie voor de aanschaf en de ontwikkeling van nieuwe producten. Voor kleine landen of leveranciers van niche-oplossingen is het nu nog lastig om een positie te verwerven in deze internationale supply chain. Dit is een knelpunt voor de export van innovatieve oplossingen voor veiligheidsvraagstukken.

- *Vraag en aanbod zijn niet transparant*
  Een belangrijke klacht van de aanbodzijde is de onduidelijkheid van de veiligheidsvraag. De overheid heeft hiervoor recentelijk een belangrijke aanzet gegeven met de formulering van kennisvragen in de subarena's voor TNO en de GTI's. De aanbodzijde is ook niet erg transparant. Leveranciers bieden vaak producten aan die in algemene zin een vergelijkbare functionaliteit hebben, maar waarvan onduidelijk is wat precies de verschillen zijn. Vaak wordt pas na aanschaf en implementatie de feitelijke functionaliteit bekend.

- *Veiligheidstechnologie bestaat niet*
  Een belangrijke constatering is dat veiligheidstechnologie niet bestaat. Er is vrijwel altijd sprake van 'andere' technologie die ook toegepast kan worden voor veiligheid. Sensoren, beeldverwerking, materialen, ICT etc. kunnen breed worden toegepast voor zowel milieu, duurzaamheid, medische systemen als ook voor veiligheid. Dit betekent dat er al veel interessant onderzoek wordt en zal worden uitgevoerd zonder dat dit afhankelijk is van een directe aansturing of (substantiële) financiering vanuit een veiligheidsoptiek. Aangezien veiligheidstechnologie niet bestaat, is er geen gemeenschappelijk nationaal onderzoeksprogramma op dit gebied. Hierdoor is de kans groot dat de kennis die op langere termijn nodig is om de maatschappelijke veiligheid te waarborgen, niet wordt ontwikkeld.

- *Er is weinig productie in Nederland*
  Er is in beperkte mate productie in Nederland. Voor een groot aantal softwaregebaseerde producten en diensten is er in Nederland wel sprake van 'productie' (softwareontwikkeling), maar dat is op beperkte schaal en vaak ook nog niet uitontwikkeld. Dit is een risico, omdat door een beperkte markt- en productieomvang in Nederland, de basis voor onderzoek en ontwikkeling afneemt. Ook het aantal buitenlandse overnames van Nederlandse bedrijven in het veiligheidsveld levert een risico voor de R&D in Nederland, omdat besluitvorming over R&D vaak in het thuisland van deze buitenlandse moederbedrijven plaatsvindt.

- *Tekort aan bèta's en technisch personeel*
  Het algemene knelpunt van een tekort aan bèta's en technisch personeel geldt in het bijzonder voor veiligheidsbedrijven. Bedrijven die zich op de defensiemarkt richten mogen alleen personeel uit NAVO-landen aannemen. En dat is internationaal gezien een krappere arbeidsmarkt. Aan de andere kant staat het onderwerp veiligheid sterk in de belangstelling en trekt het, door televisieprogramma's als Crime Scene Investigation veel aandacht. Er zijn verschillende nieuwe opleidingen van gestart, onder andere op het terrein van Forensic Science aan de Universiteit van Amsterdam.

- *Wet- en regelgeving sluiten niet altijd aan op technologische ontwikkelingen*
  Soms is wet- en regelgeving niet technologieneutraal en zijn nieuwe technologische oplossingen niet toegestaan. Of wet- en regelgeving voorziet niet in nieuwe technologische ontwikkelingen. Dit is een knelpunt bij het toepassen van innovatieve oplossingen.

- *Geen gestandaardiseerde producten*
  Voor veiligheidsproducten zijn er weinig open standaarden. Gestandaardiseerde oplossingen staan soms diametraal ten opzichte van veiligheidsvraagstukken. Bijvoorbeeld een noodknop die bij noodsituaties deuren ontsluit, kan ook gebruikt kunnen worden voor terroristische doeleinden (snel naar buiten kunnen, paniek zaaien). Om innovatie te bevorderen is het wenselijk dat er meer (open) standaarden komen, zodat deelsystemen van verschillende leveranciers met elkaar gekoppeld worden. In de toekomst kan dan eenvoudiger gewisseld kan worden van leverancier zonder (deel)systemen te vervangen.

- *Sociale, organisatorische en ethische factoren spelen een cruciale rol*
  Bij de operationele toepassing van innovatieve veiligheidsoplossingen spelen sociale, organisatorische en ethische factoren een belangrijke rol voor succesvolle toepassing. Het draait dus niet alleen om technologie.

Er zijn al vele programma's en initiatieven die raakvlakken hebben met Veiligheid

Regionaal, nationaal en internationaal bestaan diverse initiatieven die beogen kennis en innovatie op veiligheid te bevorderen en toe te passen. In de onderstaande tabel wordt een overzicht gegeven van de nationale initiatieven. Daarnaast is het Zevende Kaderprogramma van de Europese Commissie zeer relevant voor Veiligheid, omdat daarin het European Security Research Programme is opgenomen.

Tabel 0.1 *Overzicht nationale initiatieven en programma's*

Initiatief/programma	Looptijd
Sleutelgebieden aanpak / Innovatieprogramma's ministerie van Economische Zaken	
- Point-One (nano-elektronica en embedded systems)	2006 – 2009
- High Tech Automotive Systems	2007 – 2010
- Materials to innovate the industry	2008 – 2011
Maatschappelijke innovatieagenda Veiligheid (Nederland Ondernemend Innovatieland)	2008 – 2011
Innovatiegerichte onderzoeksprogramma's (IOP's)	
- Beeldverwerking	1996 – 2007
- Self Healing Materials	2005 – 2012
- Photonic Devices	2006 – 2012
- Mens-Machine Interactie	1998 - 2010
Technologie & Samenleving (met deelprogramma Veiligheid)	1995 – 2002
Maatschappelijke Sectoren & ICT (met Veiligheid als een van de thema's)	2005 – 2008
Politie en Wetenschap	Sinds 1999
Sentinels	2003 – 2011
Veilig Verbonden	Vanaf 2007
Interactive Collaborative Information Systems (ICIS)	2004 – 2009
Technologie en Opsporing	Vanaf 2004
Nationaal Platform Criminaliteitsbeheersing (NPC)	Sinds 1992
CODEMA	Tot en met 2005
Actieplan Veilig Ondernemen (AVO) – deel 1 t/m 3	Sinds 2004
Veiligheid en Beeldverwerking	Vanaf 2008
Game Research for Training and Entertainment (GATE)	Vanaf 2007
Maritieme Veiligheid	Sinds 2004
Secure Haven	Vanaf 2007

Zeven sterke Nederlandse clusters

In deze verkenning zijn zeven sterke Nederlandse clusters geïdentificeerd. Deze clusters zijn bepaald op basis van enerzijds de vraag naar innovatieve oplossingen op Defensie en Maatschappelijke Veiligheid en anderzijds het aanbod van innovatieve technologische oplossingen zoals kennis en expertise bij Nederlandse bedrijven en kennisinstellingen. Een cluster is alleen sterk als er sprake is voldoende samenhang en samenwerking en internationale excellentie. Bij het identificeren en benoemen van deze clusters is zoveel mogelijk aangesloten bij de 'capabilities' die door ESRAB benoemd zijn. Daarnaast zijn de adviezen van TNO en het NIID ter harte genomen. De clusters worden hieronder kort beschreven:

- *Detectie, identificatie en authenticatie*

  Dit cluster vindt zijn toepassing vooral in een nieuwe vorm van waarneming. Deze informatie is vervolgens input voor zowel command & control management in meldkamers als het ondersteunen van operationeel personeel op locatie. Voor een deel betreft het de 'vervanging' van 'blauw op straat' door camera's. Dit cluster heeft betrekking op

ontwikkelingen zoals (intelligent) cameratoezicht waarbij beeldanalyse wordt toegepast, zowel decentraal in de camera als centraal in de meldkamer.

- *ICT-veiligheid*
  Dit cluster richt zich zowel op de veiligheid van de ICT-infrastructuur als op de beveiliging van de informatie zelf. Het gaat hierbij niet om de inhoud van de informatie. Bij communicatienetwerken zoals internet gaat het om onderwerpen als SPAM, virussen, identificatiefraude en phishing. En bij informatiebeveiliging gaat het over onderwerpen als encryptie of virtual private netwerk ontwikkelingen (VPN).

- *Command & Control*
  Het cluster Command & Control richt zich op het operationele management bij toezicht en bij incidenten, rampen en crises. Een belangrijk aspect is de centrale aansturing vanuit één locatie waar alle relevante informatie samen komt. Naast de technologische kant is ook de menselijke factor van belang; hoe kan informatie op een passende wijze worden aangeboden, hoe moeten meldkamers optimaal worden ingericht? Verder spelen aspecten als werkdruk en stress een rol, omdat zij tot gevolg kunnen hebben dat niet alle informatie ook daadwerkelijk aandacht krijgt en/of goed wordt geïnterpreteerd.

- *Fysieke bescherming van personen en goederen*
  Het cluster heeft betrekking op het beschermen van personeel en materieel bij incidenten, aanslagen en andere gewelddadige of bedreigende situaties. Het betreft toepassingen als kogel- en steekwerende vesten voor politie en militairen, brandwerende vesten, explosiebestendig straatmeubilair (prullenbakken), catering trolleys voor vliegtuigen, containers etc.

- *Situational awareness*
  Dit cluster is gericht op het operationeel ondersteunen van veiligheidspersoneel op straat en in het veld. Niet alleen te voet, maar ook in of rond voertuigen. Het betreft mobiele en draadloze toepassingen die informatie verstrekken om beter voorbereid te zijn op incidenten waar men mee geconfronteerd zal worden. Maar ook de terugkoppeling van informatie naar de meldkamer en/of commandopost in het kader van Command & Control is van belang.

- *Onbemande waarneming*
  Het cluster Onbemande waarneming richt zich op de behoefte om verkenningen uit te kunnen voeren van incidentlocaties zonder gebruik te maken van vliegtuigen, helikopters of

het inzetten van menselijke verkenners. Het betreft toepassingen als onbemande vliegtuigen, maar ook van robotachtige voertuigen.

- *Simulatie, opleiding en training*
  Met de komst van steeds geavanceerdere oplossingen en systemen is er een toenemende behoefte aan training en opleiding. Daarnaast heeft dit cluster betrekking op simulatie en serious gaming, gericht op het virtueel oefenen voor incidenten, rampen en crises. Vanwege de wens om goed voorbereid te zijn op terroristische aanslagen is het belangrijk dat er meer operationele ervaring komt voor het goed kunnen optreden als een dergelijke situatie zich voordoet. Juist voor die situaties zijn vormen van simulatie interessant, omdat training en opleiding voor deze situaties in de praktijk niet tot nauwelijks voorkomen.

Aanbevelingen

Tot slot presenteren we een aantal aanbevelingen voor het ontwikkelen van een (maatschappelijk) innovatieprogramma rond Veiligheid. Deze aanbevelingen volgen grotendeels uit de specifieke karakteristieken van Veiligheid, kennis en innovatie en verder uit de ervaring van SenterNovem met het opzetten en uitvoeren van innovatieprogramma's. De aanbevelingen zijn:

- Volg een integrale aanpak bij het benoemen en oplossen van knelpunten;
- Versterk de relatie tussen Veiligheid en bestaande initiatieven en programma's;
- Zorg voor coördinatie;
- Sluit aan op het zevende Kaderprogramma en andere Europese programma's;

1 Inleiding

In dit hoofdstuk worden de achtergrond en de aanleiding van deze verkenning toegelicht. Vervolgens wordt ingegaan op de doelstelling en de afbakening van de verkenning. Het hoofdstuk sluiten we af met de onderzoeksverantwoording en een leeswijzer.

1.1 Achtergrond en doelstelling

Veiligheid is een van de basisbehoeften van de samenleving

Veiligheid is een van de basisbehoeften van de samenleving. De kwetsbaarheid van onze samenleving op het gebied van veiligheid is sinds het begin van deze eeuw versterkt door de aanslagen in New York, Madrid en Londen. En in algemene zin door terroristische dreigingen. Specifiek voor de Nederlandse situatie spelen de moordaanslagen op Pim Fortuyn en Theo van Gogh en de gewapende overvallen in de detailhandel een belangrijke rol.

Technologie en innovatie van groot belang voor veiligheid

Technologie en innovatie als zodanig bieden niet dé oplossing voor veiligheidsvraagstukken, maar oplossingen zonder technologie en innovatie zijn nauwelijks denkbaar. Het is dan ook wenselijk om meer gebruik te maken van de kansen en mogelijkheden die geavanceerde methoden en technieken bieden voor slimme innovatieve oplossingen om het presterend vermogen van de veiligheidsorganisaties (o.a. politie, brandweer, veiligheids- en informatiediensten) te vergroten. En zo Nederland weerbaar te houden tegen onder andere terrorisme, criminaliteit en rampen. Innovaties zijn van groot belang voor veiligheid op straat, mainports en voor het optreden van de veiligheidsorganisaties.

Nederland zet komende jaren in op innovatie en veiligheid

Het kabinet Balkenende IV in 2007 heeft in haar regeerakkoord aangegeven dat Nederland gaat inzetten op het ontwikkelen van een maatschappelijke innovatieagenda voor veiligheid. Hiervoor is een interdepartementale Programmadirectie Kennis en Innovatie ingesteld, die in haar werkprogramma het volgende aangeeft:[1]

> *"Economische en maatschappelijke doelstellingen kunnen heel goed samengaan. Het kabinet stimuleert deze kruisbestuiving door samen met belanghebbenden richtinggevende maatschappelijke innovatieagenda's uit te werken. Deze rijksbrede agenda's formuleren de ambitie van Nederland om internationaal voorop te lopen in het aanpakken van vraagstukken rondom bijvoorbeeld schone energie, goed onderwijs, duurzaam waterbeheer, gezonde voeding, goede*

gezondheidszorg, milieu, mobiliteit en veiligheid. In de aanpak zal worden aangesloten bij sterke technologiegebieden in Nederland die maatschappelijk een duidelijke relevantie hebben."

Verkenning als input voor maatschappelijke innovatieagenda Veiligheid

De doelstelling van deze verkenning is inzicht geven in de potentie van bedrijfsleven en kennisinstellingen op innovatie en veiligheid. Daarmee zal deze verkenning gebruikt kunnen worden als input voor het ontwikkelen van een maatschappelijke innovatieagenda rond veiligheid voor Nederland Ondernemend Innovatieland (NOI). Deze verkenning geeft inzicht in de sterke clusters rond Veiligheid in Nederland. Belangrijke criteria hierbij zijn de mate van samenhang en samenwerking, internationale excellentie en het (potentiële) belang van clusters voor de Nederlandse samenleving en economie. Daarnaast geeft deze verkenning een overzicht van de belangrijkste spelers in Nederland voor innovatie en veiligheid en biedt het een overzicht van relevante nationale en Europese initiatieven.

1.2 Afbakening

Met veiligheid bedoelen we 'security' en geen 'safety'

Het Nederlandstalige begrip veiligheid is heel breed. Naast 'criminele' veiligheid, wordt veiligheid ook veelvuldig gebruikt in de context van verkeersveiligheid, industriële veiligheid, arbeidsveiligheid, brandveiligheid en als consumentenveiligheid zoals ongelukjes in en om het huis. In het Engels (en het Frans) is er geen algemeen begrip voor veiligheid en wordt dit vertaald in óf 'security' in de zin van criminele veiligheid óf 'safety' dat aansluit bij de andere bovengenoemde veiligheidsbegrippen. Voor deze verkenning sluit het begrip nauw aan bij het Engelse security in de zin van criminele veiligheid waarbij er sprake is van opzettelijk, crimineel of terroristisch handelen. Preventie, voorbereiding en reactie op grootschalige incidenten, rampen en crises vallen binnen de afbakening. Hierbij is van belang om te realiseren dat rampen en crises lang niet altijd het gevolg hoeven te zijn van opzettelijk, crimineel of terroristisch handelen. Zij kunnen ook het gevolg zijn van ongelukken zoals het neerstorten van vliegtuigen, treinbotsingen, ontploffingen op raffinaderijen als ook natuurgeweld zoals overstromingen.

Veiligheid: van preventie tot crisisbeheersing

Het begrip veiligheid zoals dat in deze verkenning wordt gehanteerd omvat vraagstukken en/of toepassingen als: preventie, bescherming en optreden tegen criminaliteit en overlast, crisisbeheer-

[1] Nederland (2007b)

sing, rampenbestrijding, gecoördineerd optreden van veiligheidsdiensten, brandveiligheid, persoonlijke veiligheid van veiligheidspersoneel, terrorismebestrijding en radicalisering. Thema's als externe veiligheid, beveiliging tegen watersnood en vliegveiligheid vallen daarmee niet binnen de scope van deze verkenning. De preventie en beheersing van crises en rampen die het gevolg zijn van milieurampen, overstromingen, terroristische acties en vliegrampen, vallen echter wel binnen de scope van deze verkenning.

Innovatieve oplossingen voor zowel civiele veiligheid als voor defensie
In deze verkenning is het aanbod van oplossingen als uitgangspunt genomen. Het gaat om innovatieve en/of technologische oplossingen die zowel toepasbaar zijn voor civiele/maatschappelijke/sociale veiligheid als externe veiligheid (Defensie).[2] Er is zowel gekeken naar technologiegebieden die momenteel al veiligheidstoepassingen hebben als naar technologiegebieden die hier op dit moment nog weinig of geen toepassingen hebben, maar in potentie wel interessant zijn.

1.3 Verantwoording

Deze verkenning is geschreven door SenterNovem, onder begeleiding van een interdepartementale begeleidingsgroep bestaande uit vertegenwoordigers vanuit de ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Defensie en Economische Zaken (EZ). In de eindfase participeerde ook het ministerie van Justitie in deze begeleidingsgroep.

Als basis voor de verkenning is kennis genomen van de verschillende rapporten, studies en beleidsvoornemens die de afgelopen jaren zijn opgesteld door of in opdracht van de verschillende ministeries als ook interdepartementaal en internationaal. In dat kader is er ook aandacht voor de studies van SenterNovem die voor veiligheid zijn opgesteld. Er zijn deelonderzoeken uitgezet bij het Octrooicentrum Nederland, het Informatiecentrum van EZ en bij het TWA Netwerk van EZ. Tevens is gevraagd aan TNO, de Stichting Nederlandse Industriële Inschakeling Defensieopdrachten (NIID), Syntens en TechnoPartner om een bijdrage te leveren.

Met de verschillende studies als basis is door het projectteam een algemeen kader ontwikkeld (zie paragraaf 4.12). Vervolgens zijn er in de eerste helft van 2007 door verschillende leden van het projectteam én de begeleidingsgroep enkele tientallen gesprekken gevoerd met stakeholders. Deze gesprekken hebben primair plaatsgevonden met platforms of samenwerkingsverbanden raakvlakken

[2] In de Programmadirectie Kennis en Innovatie wordt het thema Veiligheid getrokken door de drie vakinhoudelijke ministeries BZK, Justitie en Defensie. Daarnaast is ook EZ betrokken.

hebben met het thema Veiligheid. Aanvullend is een aantal gesprekken gevoerd met individuele grotere bedrijven en met enkele grote gebruikers. Tevens hebben er gesprekken plaatsgevonden met brancheachtige organisaties als NIID en de Vereniging van Beveiligingsondernemers in Nederland (VEBON). De gesprekken waren bedoeld om een indicatief en kwalitatief beeld te krijgen van Veiligheid als mogelijk innovatiethema, en hadden niet tot doel om een (kwantitatief) compleet beeld te krijgen van het veld. Een overzicht van de stakeholders treft u aan in bijlage 1.

1.4 Leeswijzer

Deze verkenning is als volgt opgebouwd. Hoofdstuk 2 geeft een beschrijving van het veiligheidsveld. Hierbij gaan we in op vragen als: wie zijn de spelers, wat is de vraag naar veiligheid, welk aanbod op het gebied van kennis en bedrijvigheid is er, en wat zijn specifieke karakteristieken van het veiligheidsveld? In hoofdstuk 3 gaan we specifiek in op kennis en innovatie. In de eerste paragraaf geven we een uitgebreid overzicht van nationaal beleid in relatie tot veiligheid en innovatie. De tweede paragraaf gaat over het beleid van de EU en enkele van de afzonderlijke lidstaten. De laatste paragraaf van hoofdstuk 3 geeft een beeld van de zwaartepunten en excellentie op het gebied van kennis en innovatie van de Nederlandse kennisinstellingen en bedrijven. In hoofdstuk 4 presenteren we op basis van de vraag en het aanbod zeven sterke Nederlandse clusters rond Veiligheid; dit zijn clusters waar Nederland zich internationaal onderscheidt en waar voldoende samenhang en samenwerking is om een basis voor een innovatieprogramma te kunnen vormen. In hoofdstuk 5 geven we een aantal aanbevelingen. Meer gedetailleerde informatie is te vinden in de verschillende bijlagen.

2 Het veiligheidsveld in beeld

In dit hoofdstuk schetsen we een beeld van het veiligheidsveld. In paragraaf 2.1 wordt ter introductie een globaal beeld geschetst van de stakeholders die een rol spelen in het veiligheidsveld. In paragraaf 2.2 wordt vervolgens dieper in gegaan op de vraag naar veiligheidsoplossingen. In paragraaf 2.3 volgt de aanbodzijde en in paragraaf 2.4 worden de karakteristieken geschetst die de 'speelruimte' bepalen voor een innovatieprogramma rondom het thema Veiligheid.

2.1 Algemeen

In het eerste hoofdstuk is aangegeven dat veiligheid een van de basisbehoeften van de samenleving is en technologie en innovatie van groot belang zijn voor deze veiligheid. Het begrip veiligheid zoals dat in deze verkenning wordt gehanteerd is breed. Het omvat vraagstukken en/of toepassingen die betrekking hebben op het spectrum dat loopt van preventie tot crisisbeheersing. Er is een groot aantal actoren die een rol spelen bij het genereren van innovatieve en/of technologische oplossingen die toepasbaar zijn voor defensie of civiele, maatschappelijke, of sociale veiligheid. Het gaat om actoren die zich bevinden op de vraag- en aanbodzijde, om actoren die innovatieve en/of technologische oplossingen vragen, maar deze ook aanbieden. Het veiligheidsveld is met andere woorden een complexe sector. In deze verkenning komen veel van deze actoren ter sprake over hun rol en positie in veiligheid en innovatie. In deze paragraaf wordt een globaal overzicht geschetst van de belangrijkste stakeholders. In de volgende paragrafen worden de stakeholders uitvoeriger toelicht en wordt hun rol in het veld aangegeven.

Overheid

De actor overheid omvat een groot aantal overheidsinstanties die nauw betrokken zijn bij innovatie en technologische oplossingen voor veiligheidsvraagstukken. De actor overheid bestaat uit de centrale overheid zoals de ministeries van BZK, Justitie, Defensie, VWS, VROM, V&W en EZ en hun diensten zoals de politie, het Nationaal Coördinatiecentrum (NCC), de Nationaal Coördinator Terrorismebestrijding (NCTb) van BZK en de Douane van Financiën. De provincies en gemeenten vallen ook onder deze actor. De overheid is een belangrijke speler en heeft op bepaalde onderdelen een monopoliepositie zoals defensie en politie. De overheid heeft een sterke behoefte aan operationele oplossingen. Daarnaast is het veiligheidsdenken sinds de aanslag op de Twin Towers in 2001 veranderd door aandacht voor terroristische dreigingen. Het is aan de overheid de samenleving te behoeden voor grootschalige incidenten, crises en rampen, maar ook om de samenleving hierop voor te bereiden.

Kennisinstellingen en universiteiten

Kennisinstellingen en universiteiten vervullen binnen het krachtenveld de rol van aanbieder van kennis en expertise. Door het verrichten van onderzoek op uiteenlopende veiligheidsonderwerpen en participatie in internationale netwerken en projecten ontwikkelen zij kennis en producten op deze gebieden. De kennisinstellingen TNO, het Centrum voor Wiskunde en Informatica (CWI), het Nederlands Forensisch Instituut (NFI) en het Nationaal Instituut Fysieke Veiligheid Nibra (NIBRA) verrichten onderzoek naar veiligheid (zie voor een volledig overzicht bijlage 2). Naast de kennisinstellingen vindt onderzoek plaats aan dertien universiteiten. Op deze universiteiten worden door onderzoeksgroepen op verschillende thema's onderzoek verricht naar veiligheidsgerelateerde onderwerpen. Bijvoorbeeld onderzoek naar de consequenties van het aangescherpte veiligheidsbeleid voor het recht op privacy, onderzoek naar intelligente vormen van cameratoezicht of onderzoek naar nieuwe materialen voor steek- en kogelwerende kleding. De universiteiten vervullen verder een rol in het onderwijzen van studenten op aan veiligheid gerelateerde onderwerpen.

Bedrijven

Er zijn ruim vijfhonderd bedrijven direct actief op de veiligheidsmarkt.[3] Dit zijn zowel startende bedrijven, bijvoorbeeld spin-offs van universiteiten, als grote bedrijven zoals Philips en Thales. De bedrijven vervullen in het krachtenveld allereerst de rol van aanbieder. Bedrijven werken bijvoorbeeld samen met kennisinstellingen of universiteiten aan de ontwikkeling van nieuwe producten en diensten. Dit varieert van draaideuren tot de bewaking van bedrijventerreinen. Bedrijven zijn ook een vragende partij, namelijk als slachtoffer van criminaliteit. Samen met de overheid werkt het bedrijfsleven binnen het Nationaal Platform Criminaliteitsbeheersing (NPC, zie hoofdstuk 3) aan oplossingen om het bedrijfsleven hiertegen meer weerbaar tegen te maken.

Overigen

Andere organisaties die een rol spelen zijn bijvoorbeeld brancheorganisaties, publiekprivate samenwerkingen en dienstenleveranciers. De rollen van de brancheorganisaties verschillen qua karakter, rol en activiteiten. De NIID heeft bijvoorbeeld een rol voor de Nederlandse defensiegerelateerde industrie. Het Verbond van BeveiligingsOndernemingen (VvBO) en de VEBON hebben daarentegen als achtergrond de dienstverlening voor private surveillanten, beveiligers en de alarmeringsproducten en –dienstverlening. Andere brancheorganisaties zijn het ICT~Office en de Federatie van Technologiebranches (FHI). Bij de publiekprivate samenwerking gaat het om het Centrum voor Criminaliteitsbeheersing en Veiligheid (CCV), het NPC en het Electronic Commerce Platform

[3] Inschatting op basis van SenterNovem (2004, 2007) en Research voor Beleid (2004)

Nederland (ECP.NL). Deze organisaties richten zich wel op maatschappelijke veiligheid, maar niet specifiek in combinatie met innovatie. [1] Omdat het aanbod van oplossingen vaak niet direct door de gebruiker 'zelf' kan worden ingezet, spelen dienstenleveranciers een rol in het veld. Zij bieden innovatieve oplossingen aan, vaak als onderdeel van een breder servicepakket aan de eindgebruiker. Voorbeelden van deze leveranciers zijn beveiligingsinstalleurs en systeemintegrators.

2.2 Vraag

In de vorige paragraaf hebben we het krachtenveld op het gebied van veiligheid besproken. In deze paragraaf gaan we in op de maatschappelijke vraag naar veiligheidsoplossingen die door de centrale overheid is geformuleerd. Eerst wordt aandacht geschonken aan de defensievraag en vervolgens de vraag vanuit maatschappelijke veiligheid.

Defensie

De vraag van Defensie is het laatste decennium sterk van karakter veranderd. Deze verandering hangt samen met de veranderde taak voor Defensie. In het verleden was de vraag van Defensie gericht op technologische en innovatieve oplossingen voor de verdediging van Nederland door de dreiging van de Koude Oorlog. Met het wegvallen van deze dreiging vraagt Defensie tegenwoordig naar oplossingen die gerelateerd zijn aan vredesoperaties. Bovendien is er sprake van meer internationale samenwerking waarbij Nederland specifieke 'capabilities' inbrengt. De nadruk ligt niet alleen meer op het kunnen optreden in het hoogste geweldsspectrum, maar heeft een meer civiel karakter heeft gekregen richting een opbouwmissie en het bewaken van de openbare orde. In militaire kringen wordt dit aangeduid als 'Modus Operandi Other Than War' (MOOTW).

Defensie is benoemd als één van de twaalf arena's in het advies van de Commissie Wijffels voor de vraagsturing TNO en de groot technologische instituten (GTI's).[4] Het ministerie van Defensie is regievoerder van het gelijknamige thema van de maatschappelijke arena. Binnen deze arena zijn er achttien subthema's benoemd, zie Tabel 1.

[4] Ad Hoc Commissie "Brugfunctie TNO en GTI's" (2004)

Tabel 1 *Subthema's Arena Defensie (bron: Ministerie van OCW, 2006)*

Subthema's Arena Defensie		
1. Future Operations & Technology	7. NBC	13. Doelmatigheid en bedrijfsvoering
2. Joint Air Defense	8. Bescherming en beveiliging	14. Inlichtingen
3. C4I	9. Man in het veld	15. Land optreden en systemen
4. Sensoren	10. Menselijk presteren	16. Lucht optreden en systemen
5. Munitie	11. Opleiding en training	17. Maritiem optreden en zeesystemen
6. Onderwater Oorlogsvoering	12. Modeling en simulation	18. Overig

Door de hierboven beschreven ontwikkelingen heeft Defensie behoefte aan nieuwe capaciteiten, met op hun beurt nieuwe innovatiekarakteristieken. De ontwikkeling van grootschalige oorlogsvoering naar kleinschaliger missies met vele onzekerheden heeft ertoe geleid dat mensen en materieel op zeer uiteenlopende situaties voorbereid moeten zijn. De toenemende samenwerking met andere partijen binnen deze missies stelt verder eisen aan standaardisatie en communicatie. Een ander aspect is de steeds duidelijker wordende noodzaak slachtoffers aan beide kanten zoveel mogelijk te vermijden. TNO onderscheidt de volgende belangrijke innovatiekarakteristieken voor Defensie:[5]

1. Versterking van de informatiebehoefte;
2. Alomtegenwoordige aanwezigheid van informatie;
3. Genetwerkte koppeling tussen mensen en materieel;
4. Flexibel, mobiel, kleinschalig en modulair;
5. Betrouwbaar, robuust en goed beschermend materieel;
6. Personeel dat goed getraind is op het nieuwe materieel en de nieuwe vormen van optreden;
7. Precisie en effectiviteit;
8. Onbemand, autonoom en op afstand;
9. Logistieke en economische efficiëntie.

Naast deze innovatiekarakteristieken worden in deze studie een drietal trends genoemd. Deze zijn geformuleerd op basis van de voor Defensie essentiële technologiegebieden. Een eerste trend is verschuiving van langetermijn R&D naar kortetermijnontwikkeling. De tweede trend is het toenemende belang van wapensysteemmanagement en instandhouding. De derde trend is de verschuiving van de rol van Defensie van co-maker naar lead-user. Voor de realisatie zijn de volgende technologieën van groot belang:[6]

[5] TNO (2006)
[6] Ministerie van EZ en Defensie (2007)

1. Command, Control, Communication, Computers & Intelligence (C4I);
2. Sensorsystemen;
3. Geavanceerde materialen;
4. Elektronica en mechatronica;
5. Bescherming en wapensystemen;
6. Geïntegreerd systeemontwerp en –ontwikkeling.

Maatschappelijke Veiligheid

Maatschappelijke Veiligheid is ook benoemd als één van de twaalf arena's in het advies van de Commissie Wijffels. Het ministerie van BZK is regievoerder van dit thema en zorgt voor de interdepartementale afstemming en aansluiting op het Europese R&D-programma (ESRP/Europese zevende Kaderprogramma, zie hoofdstuk 3).

In het verlengde van zowel de vraagsturing TNO/GTI's als het advies van het European Security Research Advisory Board (ESRAB) uit 2006[7] is besloten om met een nationaal R&D-programma op het gebied van maatschappelijke veiligheid te komen. Dit programma is momenteel in ontwikkeling en heeft de acht subthema's (ook wel subarena's genoemd) van de arena Maatschappelijke Veiligheid als basis.[8] Deze subthema's worden in Tabel 2 gepresenteerd. Als basis voor dit R&D-programma is naast de vraagsturing TNO/GTI's en het ESRAB advies bovendien nadrukkelijk gekeken naar wat Maatschappelijke Veiligheid van Defensie kan leren. TNO heeft in 2006 een studie afgerond waarin is gekeken naar de technologieontwikkeling bij Defensie en de trends die van belang zijn voor Maatschappelijke Veiligheid.[9] Er is ook een interdepartementale werkgroep geweest die gekeken heeft naar meer samenwerking tussen Defensie en BZK.[10] Naast een meer algemene onderbouwing voor het R&D-programma Maatschappelijke Veiligheid heeft dit onder meer geleid tot operationele afspraken voor het gebruik van defensiematerieel bij rampen en crises en meer samenwerking tussen de veiligheidsregio's en de Regionaal Militaire Centra (RMC).

Tabel 2 *Subthema's Maatschappelijke Veiligheid (bron: **www.veiligdoorinnovatie.nl**)*

Subthema's Arena Maatschappelijke Veiligheid	
1. Terrorisme & radicalisering	5. Versterking opsporing & handhaving
2. Dreiging-/risicoherkenning & analyse	6. Versterking crisisbeheersing
3. Veel voorkomende criminaliteit & overlast	7. Geïntegreerde systemen
4. Veiligheid van netwerksystemen	8. Uitrusting & materieel

[7] Europese Commissie (2006)
[8] zie www.veiligdoorinnovatie.nl
[9] TNO (2006b)
[10] Ministerie van BZK en Defensie (2005, 2006)

Veiligheid is verder één van de vijf pijlers van het beleidsprogramma van het kabinet Balkenende IV.[11] Voor technologieontwikkeling voor het veiligheidsbeleid en voor innovatie en kennisopbouw voor de langere termijn vanuit het perspectief van Nederland Ondernemend Innovatieland, heeft het kabinet 54 miljoen euro beschikbaar voor investeringen in de kabinetsperiode 2007-2011.[12] In Tabel 3 is de relatie tussen de beleidsprioriteiten op het domein veiligheid en de subthema's uit de Arena Maatschappelijke Veiligheid weergegeven.[13]

Tabel 3 *Beleidsprioriteiten 2007-2011 versus subthema's Arena Maatschappelijke Veiligheid*

Beleidsprioriteiten 2007-2011	Subthema's Arena Maatschappelijke Veiligheid
1.2 Krachten bundelen voor vrede, veiligheid en ontwikkeling	Dreigings-/ risicoherkenning & analyse
	Veiligheid van netwerksystemen
	Uitrusting & materieel
4.5 Naar 40 krachtwijken	Veel voorkomende criminaliteit & overlast
5.2 Aanpak van agressie, geweld, diefstal en criminaliteit tegen ondernemingen	Veel voorkomende criminaliteit & overlast
5.3 Aanpak overlast en verloedering	Veel voorkomende criminaliteit & overlast
5.4 Identiteitsvaststelling, technologie en informatie-uitwisseling	Versterking opsporing & handhaving
	Veel voorkomende criminaliteit & overlast
	Geïntegreerde systemen
5.5 Bestrijding van vormen van ernstige criminaliteit	Versterking opsporing & handhaving
	Veiligheid van netwerksystemen
5.6 Terrorismebestrijding en tegengaan radicalisering	Terrorisme & radicalisering
	Versterking crisisbeheersing
5.7 Effectieve organisatie van de veiligheidsketen	Geïntegreerde systemen
	Uitrusting & materieel
5.8 Crisisbeheersing en rampenbestrijding	Versterking crisisbeheersing
	Geïntegreerde systemen

Binnen de onderscheiden behoeften voor Maatschappelijke Veiligheid neemt het onderwerp ICT-veiligheid een aparte plaats in. Dit onderwerp is heeft een ander karakter dan de meeste overige veiligheidsonderwerpen. Het is belangrijk hierbij onderscheid te maken tussen:

- *ICT-voor-Veiligheid:* de toepassing van ICT zoals bijvoorbeeld beeldverwerking, intelligente camera's, integratie van sensoren, databases, datamining;
- *Veiligheid-van-ICT:* de veiligheid van de ICT-infrastructuur.

De veiligheid-van-ICT is voor onze maatschappij in toenemende mate belangrijk. Onze maatschappij en vele sectoren van onze economie zijn in hoge mate afhankelijk van de ICT-infra-

[11] Nederland (2007)
[12] Nederland (2007b)
[13] Op basis van Nederland (2007) en Ministerie van BZK (2007)

structuur. Deze ICT-afhankelijkheid speelt nadrukkelijk een rol bij onze nationale veiligheid en de vitale infrastructuur. ICT loopt horizontaal door onze maatschappij en economie, daarom heeft het interdepartementale project 'Herijking ICT Veiligheidsbeleid' in 2006 aandacht geschonken aan de rol van de overheid voor ICT-veiligheid. In juli 2007 is de rapportage van dit project aan de Tweede Kamer aangeboden en is toegezegd eind 2007 te komen met een beleidsagenda.[14] In mei 2007 verscheen daarnaast van ICTRegie een rapport waarin de onderzoeksagenda is geschetst die nodig is om de veiligheid van ICT-netwerken te optimaliseren.[15] Een aspect van ICT-veiligheid is Cyber Crime. Zowel nationaal als internationaal is hier veel aan-dacht voor. Vooral omdat het een internationale vorm van criminaliteit is die geen grenzen kent. Voor de Europese Commissie is Cyber Crime een aandachtsgebied.[16] Er wordt duidelijk onderscheid gemaakt tussen drie soorten van Cyber Crime: traditionele criminaliteit in een nieuw jasje (zoals fraude), verspreiding van illegale inhoud via digitale netwerken en specifieke elektronische vormen van criminaliteit zoals criminaliteit gericht tegen de ICT-infrastructuur (denial-of-service).

2.3 Aanbod

In verschillende studies zijn de defensiegerelateerde en veiligheidsindustrie in kaart gebracht. In deze paragraaf gaan we in op de kenmerken van deze beide industrieën en komen de sterkten en zwakten aan bod. Tot slot van deze paragraaf bespreken we de kennisinstellingen en universiteiten.

Defensiegerelateerde industrie

In 2004 heeft Research voor Beleid een sectoranalyse van de Nederlandse defensiegerelateerde industrie uitgevoerd.[17] Deze studie laat zien dat er in totaal 245 bedrijven actief zijn die zich bijna allemaal ook richten op civiele activiteiten. De bedrijven zijn vaak onderdeel van grotere organisaties met een internationale oriëntatie. De bedrijven zijn het meest actief op de terreinen: lucht- en ruimtevaart, marinebouw, commando, controle- communicatie- en informatietechnologie. In 2002 had de industrie een omzet van 1,72 miljard euro (4% van de totale omzet van de betrokken bedrijven). De industrie heeft een sterke internationale focus: 72% van de bedrijven verricht werkzaamheden voor het buitenland en 45% van de omzet komt voor rekening van exportactiviteiten. Grote, kleine en middelgrote bedrijven zijn actief in het buitenland. Vooral in Duitsland, de Verenigde Staten, België en het Verenigd Koninkrijk. Uit het onderzoek komt verder naar voren dat deze

[14] Ministerie van EZ, BZK en Justitie (2007)
[15] ICTRegie (2007)
[16] Europese Commisie (2007b)
[17] Research voor Beleid (2004)

industrie 11.000 arbeidsplaatsen telt, waarvan eenderde R&D-arbeidsplaatsen. In Tabel 4 zijn de kerncijfers opgenomen.

Tabel 4 *Kerncijfers defensiegerelateerde industrie (bron: Research voor Beleid, 2004)*

Kerncijfers defensiegerelateerde industrie	2002
Aantal bedrijven	245
% defensiegerelateerde bedrijven met civiele werkzaamheden	91%
Defensiegerelateerde omzet	EUR 1,72 miljard
Defensiegerelateerde omzet als % van de totale omzet	4%
Omvang export	EUR 0,77 miljard
Defensiegerelateerde werkzame personen	12.000
Defensiegerelateerde arbeidsplaatsen	11.000
Defensiegerelateerde R&D-arbeidsplaatsen	3.500

De industrie is qua omvang en direct economisch belang beperkt, echter, de omzet per medewerker is hoger dan het gemiddelde. Indirect is de industrie wel van belang. De industrie kent een hoog technologisch karakter met belangrijke spill-over effecten.

De studie van Research voor Beleid geeft verder aan dat Nederlandse bedrijven en kennisinstellingen een sterke kennis- en technologiepositie hebben. De onderdelen marineschepen, radartechnologie en onderdelen van de luchtvaart en simulatie worden hoog aangeslagen. Als belangrijkste sterkte van de defensiegerelateerde industrie wordt het kunnen voortbrengen van technologisch hoogwaardige kennis en producten genoemd. Een ander sterk punt, dat tevens ook een zwak punt is betreft de specialisatie van bedrijven op bepaalde niches. Twee minder sterke punten van deze industrie zijn de beperkte schaalgrootte (minder dan de helft van de bedrijven heeft een defensie-omzet van meer dan een miljoen euro) en de versnippering in de productieketen. Met de versnippering wordt bedoeld dat defensieactiviteiten zeer verschillend zijn en vaak niet op elkaar aansluiten.

TNO heeft op basis van deze studie de sterke kanten van de defensiegerelateerde industrie nader onderzocht.[18] Deze analyse heeft vervolgens als basis gediend voor de Defensie Industrie Strategie (DIS), die in 2007 door de ministeries van EZ en Defensie is gepubliceerd.[19] Uit de analyse van TNO komt naar voren dat de Nederlandse industrie een sterke positie heeft op acht technologie- en toepassingsgebieden: Command, Control, Communication, Computers en Intelligence (C4I); Sensorsystemen; Elektronica en mechatronica; Aandrijving en energiesystemen; Geavanceerde mate-

[18] TNO (2006)
[19] Ministeries van EZ en Defensie (2007)

rialen; Mechanica en hydraulica; Geïntegreerd systeemontwerp- en ontwikkeling; en Simulatie, training en kunstmatige omgevingen.
Wanneer vraag en aanbod aan elkaar gerelateerd worden, wordt duidelijk dat de grootste kansen voor de Nederlandse defensiegerelateerde industrie, liggen bij de clusters C4I en Sensorsystemen. Op deze twee gebieden is de industrie sterk en lijken interessante kansen aanwezig, ook voor wat betreft de civiele markt. Een iets minder sterke positie, met wel sterke niche-posities, heeft de industrie op de volgende technologieclusters: geïntegreerd systeemontwerp en -ontwikkeling; elektronica en mechatronica; geavanceerde materialen; en simulatie, training en kunstmatige omgevingen. Op drie technologieclusters (aandrijving en energiesystemen; bescherming en wapensystemen; en mechanica en hydraulica) heeft de Nederlandse industrie geen uitzonderlijk sterke positie en zijn de nationale en internationale defensie en civiele kansen relatief beperkt.

Figuur 1 biedt een overzicht van de sterke en zwakkere clusters binnen de defensiegerelateerde industrie. In deze figuur wordt een onderscheid gemaakt tussen drie typen technologieclusters:

- Type 1 technologieclusters zijn de brede, sterke clusters, waarin zowel vraag als aanbod goede potentie bieden voor de industrie;
- Type 2 clusters zijn wat minder breed vertegenwoordigd, maar hierin bevindt zich een niet onaanzienlijk aantal (potentiële) nichekansen, die een beperkt, maar significant karakter hebben;
- Type 3 cluster hebben een gefragmenteerd, nichekarakter. Vraag en aanbod bieden een wisselend perspectief.

Figuur 1 *Spiegeling van sterkten en zwakten (bron: TNO, 2006)*

		Onderdelen			
	Technologie clusters	Sterkten NL-DGI	Internationale ontwikkelinger	Behoeften defensie	Civiele kansen
Type 1	C4I	++	++	++	++
	Sensorsystemen	+	++	++	++
Type 2	Geïntegreerd systeemontwerp en -ontwikkeling	+	+	+	+
	Elektronica en mechatronica	(+)	(+)	+	+
	Geavanceerde materialen	(+)	(+)	+	+
	Simulatie, training en kunstmatige omgevingen	+	(+)	+	+
Type 3	Aandrijving en energiesystemen	+	0	(+)	0
	Bescherming en wapensystemen	0	0	+	0
	Mechanica en hydraulica	+	0	0	0

++	Een breed vertegenwoordigd cluster van technologieën.
+	Clusters met een wat meer nichekarakter met een aanzienlijk aantal niches.
(+)	Cluster waarbij de discussie met experts, literatuur en eigen expertise, de sterkten/kansen significant afwijken van de analyse van de enquêtes. Dit zal in
0	Een minder significant, fragmentarisch cluster.

Veiligheidsindustrie

Voor de veiligheidsindustrie zijn geen uitgebreide cijfers beschikbaar zoals bij de defensiegerelateerde industrie. Uit onderzoek naar defensiegerelateerde industrie van Research voor Beleid blijkt het overgrote deel van de 245 bedrijven ook actief zijn op de civiele markt. Uit een inventarisatie van SenterNovem naar R&D in security (exclusief defensiegerelateerd onderzoek) in 2007, blijkt dat 342 bedrijven R&D verrichten op dit gebied (in de periode 2003-2005).[20]

Ondanks het ontbreken van een duidelijk beeld van grootte en aard van deze industrie, zijn er drie studies uitgevoerd naar de kansen van de veiligheidssector. Dit zijn een verkenning van SenterNovem[21] en een studie van RAND Europe[22] naar R&D-activiteiten in Nederland op het gebied van ICT & Veiligheid.[23] SenterNovem en RAND Europe brengen de kansrijke gebieden en sterke

[20] SenterNovem (2007)
[21] SenterNovem (2005)
[22] RAND Europe (2004)
[23] In het kader van het project Digibewust heeft ECP.nl in 2007 een actualisatie uitgevoerd van deze studies (zie ECP.NL, 2007)

onderzoeksvelden in kaart op het gebied van ICT-veiligheid. Daarnaast heeft TNO op verzoek van het projectgroep een korte studie uitgevoerd over de veiligheidsgerelateerde industrie.[24] Het Senter-Novem-onderzoek wijst zeven kansrijke gebieden aan (zie Tabel 5). Uit deze tabel blijkt dat er binnen deze zeven kansrijke gebieden een onderscheid wordt gemaakt in de Nederlandse kennispositie. Daarnaast wijst de studie twee gebieden aan met een hoge potentie, maar deze hebben weinig of een matige R&D-industrie in Nederland. Het betreft de gebieden: Cryptografie en Radartechnologie.

Tabel 5 *Kansrijke gebieden op het gebied van ICT-veiligheid (bron: SenterNovem, 2005)*

Kansrijk gebied	Kennispositie NL
Network security	Zeer goed
E-commerce, e-business, PKI, digitale handtekening, data privacy, Smartcards	Zeer goed
Digital Rights Management, Digital Watermarking, digital copyright, content protection	Redelijk tot goed
Tracking & tracing: Location Based Services	Redelijk tot goed
Biometrie	Redelijk
Intelligente camera's, computervision/beeldverwerking, video/audio-analyse (sensor datafusie)	Redelijk
Cybercrime	Matig tot redelijk

Het onderzoek van RAND Europe beschrijft een zeer sterke concurrentie op de wereldmarkt voor informatie- en netwerkveiligheid. De voornaamste markt zijn de Verenigde Staten. Echter, Europa presteert op bepaalde gebieden sterker (smartcards en privacy). Ondanks enkele sterke onderzoeksvelden is Nederland op bepaalde onderwerpen te klein om een rol van betekenis te spelen. De kleine omvang beperkt Nederland om te participeren in internationale consortia, ook al is de internationale oriëntatie van bedrijven en kennisinstellingen goed. In Tabel 6 zijn de sterke en zwakke onderzoeksvelden en de kansen en bedreigingen weergegeven. De sterke onderzoeksvelden cryptografie en privacy behoren tot de zwaartepunten van het huidige internationale onderzoek en zullen naar verwachting groeipolen zijn voor het ICT-onderzoek in de komende jaren. De specifieke onderzoeksvelden waarin Nederland minder sterk is, zijn minder belangrijk voor de ontwikkeling van de informatiesamenleving. Verder concluderen de onderzoekers dat de kansen van de Nederlandse R&D voor Digital Rights Management en biometrie eveneens toekomstige groeipolen zijn. Indien deze kansen goed worden benut, is het de verwachting dat Nederland op dit terrein een vooraanstaande rol kan spelen.

[24] TNO (2007)

Tabel 6 *Overzicht sterke, zwakke, kansen en bedreigingen onderzoeksvelden ICT-veiligheid (bron: Rand Europe, 2004)*

Sterke onderzoeksvelden	**Zwakke onderzoeksvelden**
Smartcards	IT-security tools
Cryptografie	Ondersteunende disciplines
Privacy	
Beleidsanalyse en veiligheidsconsultancy	
Kansen	**Bedreigingen**
Digital Rights Management en watermarking	Naar het buitenland verdwijnen van cryptologie.
Biometrie	Toenemende kennisachterstand smartcardontwikkeling.
Cybercrime	Ontwikkeling nieuwe technologieën onvoldoende vertaald
Authenticatie	naar praktische toepassingen.

Tegenover deze positieve conclusies staan twee bedreigingen. Allereerst wordt gewezen op de zwakke implementatie van de R&D-resultaten. Een tweede punt is dat het cryptografisch onderzoek voor een deel naar het buitenland verdwijnt. En dat Nederland krachtig is in verificatie en certificering van smartcards en niet in technologische ontwikkeling. De sterkten en kansen kunnen volgens RAND Europe alleen worden benut als het institutionele en financiële kader van R&D gezond is. Er wordt echter gewezen op een drietal structurele problemen:

- De onderzoekscapaciteit van het bedrijfsleven in de ICT-sector is sinds de jaren negentig sterk afgenomen en zowel publieke als particuliere sectoren lijden aan een gebrek aan onderzoekers;
- De samenwerking tussen industrie, overheid en kennisinstellingen schiet tekort;
- Onderzoek en beleid hebben behoefte aan betere coördinatie. Er is weinig samenhang in onderzoeksactiviteiten van universiteiten en het overheidsbeleid voor ICT is verspreid over meerdere ministeries en departementen.

Op verzoek van de projectgroep heeft TNO het Nederlandse bedrijfsleven in beeld gebracht dat een belang heeft bij het thema Veiligheid.[25] TNO onderscheidt vier categorieën van bedrijven en geeft aan waar het Nederlandse bedrijfsleven een internationaal onderscheidende positie heeft of kan opbouwen (in Tabel 7 zijn per categorie alleen de producten en diensten opgenomen waar het bedrijfsleven een onderscheidende rol heeft of kan opbouwen).

[25] TNO (2007)

Tabel 7 *Bedrijfsleven met een belang bij het thema Veiligheid (bron: TNO, 2007)*

Categorie bedrijfsleven met belang bij Veiligheid	**Producten en diensten**	**Voorbeelden van Nederlandse bedrijven**
Leveranciers van geavanceerde technologische producten en systemen ("maatwerkoplossingen" voor veiligheidsproblemen	Mulit-sensorsystemen (elektro-optische sensoren, radar, camera's)	Thales, Smith Detection, Philips, Astron, Eaton/Holec, HITT, leden FHI
Leveranciers van materialen, apparaten en installaties (in bulk cq. Seriematig geproduceerde goederen)	Beschermende materialen	DSM, Ten Cate, Dijkstra, Corus, Futura Composites, Dupont, Gammaholding, 3M, Dräger, MSA, vele MKB's, Sioen, Seyntex
	Navigatie-apparatuur voor first responders	TomTom, Siemens
	Beveiligingssystemen (incl. alarminstallaties, meldkamers)	Leden UNETO-VNI (ca. 350 MKB's), Kropman, Tyco, Imtech, GTI, Initial Varel
Leveranciers van commerciële diensten	Beveiligingsdiensten	Securitas, Securitae, Trigion, Falck, G4S, Prened, SSON, Geofencing
	Training en opleiding	Trigion, vele MKB's
	Consultancy veiligheid	DHV, Arcadis, KPMG, Honeywell, Twijnstra Gudde
	Intelligence-diensten	
Bedrijven, waarvoor Veiligheid een concurrentiekracht cq. continuïteit bepalende "enabler" is	Bouw van kritische civiele infrastructuur (bijv. bruggen, tunnels, havens, kabels en netwerken)	Volker Stevin, Mecon Engineering, Casema
	Goederentransport (zee, lucht, weg)	Havenbedrijf Rotterdam, Schiphol, Op- en overslagbedrijven Rotterdam
	Financiële sector (incl. banken)	ABN-AMRO, ING

Kennisinstellingen en universiteiten

Het totale overzicht van Nederlandse kennisinstellingen en universiteiten die actief zijn op het terrein van Veiligheid is opgenomen in bijlage 2. De belangrijkste conclusies zijn:

- Onderzoek vindt plaats aan 13 universiteiten (Erasmus Universiteit Rotterdam, Universiteit van Tilburg, Radboud Universiteit, Universiteit Leiden, Technische Universiteit Delft, Technische Universiteit Eindhoven, Universiteit van Utrecht, Rijksuniversiteit Groningen, Universiteit Twente, Universiteit van Amsterdam, Vrije Universiteit Amsterdam en Wageningen Universiteit);
- De volgende relevante kennisinstellingen zijn geïdentificeerd: TNO, CWI, NFI, NIBRA, Instituut voor Voedselveiligheid (RIKILT), Rijksinstituut voor Volksgezond en Milieu (RIVM), Nationaal Lucht- en Ruimtevaartlaboratorium (NLR), Netherlands Institute for Metals Research (NIMR), Embedded Systems Institute (ESI) en Telematica Instituut. Een bijzondere positie is er voor TNO. Hier zijn alleen al voor het onderdeel TNO Defensie en

Veiligheid 1.060 personen werkzaam. Daarnaast hebben andere TNO-onderdelen als ICT of Kwaliteit van Leven ook veiligheidsgerelateerde eenheden.

- Uit het overzicht[26] van HBO-opleidingen op het gebied van Veiligheid komt naar voren dat vijf lectoren zich toeleggen op dit gebied. Het betreft de lectoraten Risicobeheersing (Saxion), Veiligheid en Sociale Cohesie in het publieke domein (Windesheim), Veiligheid, Sociale veiligheid en Fysieke Veiligheid (Hogeschool Zeeland). Daarnaast houdt ook de Politieacademie zich bezig met dit onderwerp.

2.4 Karakteristieken

Deze karakteristieken van het veiligheidsveld zijn uiteenlopend van aard. Het betreft een zeer specifiek kenmerk van de sector, het zijn sterke punten of kansen of het zijn knelpunten. Het onderstaande overzicht is tot stand gekomen op basis van de verschillende studies en de interviews, maar zal niet volledig zijn. Een aantal karakteristieken geldt ook voor andere onderdelen van de Nederlandse economie, maar zijn toch meegenomen omdat ze voor Veiligheid in grotere mate gelden. Tevens zijn twee karakteristieken opgenomen die vooral voor Defensie gelden, maar ook een uitstraling hebben naar de veiligheidsgerelateerde industrie. De karakteristieken zijn:

- Overheid is zelf een grote speler en belangrijk als eerste klant.
- Er is een trend van ‘made to measure’ naar ‘commercial of the shelf’ (COTS).
- Er is een wereldmarkt, maar grote landen hebben nog afgeschermde markten.
- Vraag en aanbod zijn niet transparant.
- Veiligheidstechnologie bestaat niet.
- Er is weinig productie in Nederland.
- Tekort aan bèta’s en technisch personeel.
- Wet- en regelgeving sluit niet altijd aan op technologische ontwikkelingen.
- Geen gestandaardiseerde producten.
- Sociale, organisatorische en ethische factoren spelen een cruciale rol.

Overheid is zelf een grote speler en belangrijk als eerste klant

Eén van de meest kenmerkende karakteristieken van de veiligheidssector is dat de overheid zelf een belangrijke speler is. Voor andere thema’s zoals onderwijs of de zorg is de overheid weliswaar direct verantwoordelijk, maar wordt de uitvoering overgelaten aan scholen, universiteiten, ziekenhuizen, verzorgingstehuizen etc. Voor Veiligheid is de overheid echter zelf de uitvoerder. Voor een aantal taken heeft de centrale overheid zelf een monopolistische positie zoals politie, defensie en

[26] Informatiecentrum EZ (2007b)

veiligheidsdiensten. In het openbare leven is er echter sprake van een zeer sterk toegenomen aanwezigheid van particuliere beveiligers. Voor andere taken heeft de centrale overheid vooral een faciliterende rol, zoals bij de brandweer. Pas als er sprake is van grootschalige incidenten, crises of rampen heeft de centrale overheid een coördinerende rol.

Deze specifieke positie en rol van de (centrale) overheid betekent dat er voor innovatie specifieke kaders van toepassing zijn. Voor een deel vertaalt zich dat in een sterke focus op veiligheidsvragen die 'nu' spelen met een sterke behoefte aan concrete en operationele oplossingen ('commercial-of-the-shelf', zie volgende paragraaf). De overheid kan als 'launching customer' bijdragen aan het sneller realiseren en toepassen van innovatieve oplossingen. Bij de eerste toepassing van oplossingen is er immers nog de nodige onzekerheid over de operationele robuustheid. Het realiseren van een stand-alone situatie is anders dan een geïntegreerde oplossing als onderdeel van een complex systeem en de uitrol naar een sectorbrede toepassing. Wanneer de overheid optreedt als laucnhing customer moet de oplossing primair gericht zijn op in Nederland ontwikkelde producten en oplossingen en/of op de Nederlandse kennisinfrastructuur betrekking hebben. Bovendien is het voor Nederlandse producenten belangrijk voor de internationale uitrol dat men kan aangeven dat de Nederlandse overheid al gebruiker is van het product.

Voor Maatschappelijke Veiligheid is de overheid niet de enige partij die veiligheidstaken uitvoert. Bedrijven en burgers zijn zelf verantwoordelijk voor een belangrijk deel van hun eigen veiligheid. Bij meer serieuze veiligheidsrisico's wordt dit door commerciële dienstverlening professioneel ingevuld door surveillanten en beveiligers, alarmopvolging, alarmcentrales etc. Innovatievraag en -behoefte liggen dan niet alleen bij de overheid maar ook bij bedrijven en burgers.

Er is een trend van 'made to measure' naar 'commercial of the shelf' (COTS)

Voor de aansturing en samenwerking van defensiegerichte innovatie is er de laatste decennia een duidelijke verandering zichtbaar. Voorheen was er veelvuldig sprake van 'made to measure'. Defensie was nauw betrokken bij de vraagformulering en het ontwikkelingstraject en was ook 'bij afspraak' koper van de operationele oplossingen. Hierdoor was het bedrijfsleven zeker van de overheid als klant. Dit gaf een basis voor zowel het daadwerkelijk in productie nemen van operationele oplossingen als ook het commercieel kunnen exporteren van die producten en diensten.

De laatste jaren staat Defensie niet meer automatisch garant voor de aanschaf. Vanuit Defensie zijn er wel wensen en is er de wil om mee te denken. Defensie wil echter niet meer gebonden zijn en wil kunnen kiezen uit oplossingen die commercieel beschikbaar zijn. Een andere ontwikkeling is dat specifieke defensieopdrachten onvoldoende zijn om productie te rechtvaardigen. In toenemende mate leidt dit tot een situatie dat er eerst een voldoende grote niet-defensiemarkt moet zijn om

commerciële productie te rechtvaardigen. Deze ontwikkeling wordt aangeduid als 'commercial of the shelf' (COTS).

Voor de Nederlandse defensiegerichte industrie, waarvan onderdelen een hechte relatie hadden met Defensie, is deze ontwikkeling nieuw. De COTS-invalshoek spreekt hen aan, maar de automatische thuismarkt ontbreekt waardoor opdrachten in een internationaal krachtenspel verworven worden. De defensiebehoefte is en blijft aanwezig, maar in een meer open markt. Deze ontwikkeling past in het nationale en Europese beleid voor meer marktwerking en de eerder genoemde internationale supply chain.

Ook voor toepassingen in de sfeer van Maatschappelijke Veiligheid is deze COTS-karakterisering belangrijk. De (overheid gestuurde en gecoördineerde) innovatievraag is nog relatief nieuw en in ontwikkeling. Een vanuit COTS-perspectief overheidsgestuurde maatschappelijke innovatievraag kan echter slechts onderdeel zijn binnen een breder commercieel en economisch marktperspectief voor de ontwikkelaars. Dit heeft als gevolg dat oplossingen niet gerealiseerd kunnen worden met alleen de (centrale) overheid als klant.

Er is een wereldmarkt, maar grote landen hebben nog afgeschermde markten

De defensiemarkt ontwikkelt zich naar een wereldmarkt, dat betekent meer marktwerking en producten worden wereldwijd beschikbaar en verkocht.[27] Er is sprake van een internationale supply chain. Op dit moment is er echter nog geen 'level playing field'. In Verenigde Staten, Verenigd Koninkrijk, Frankrijk, Duitsland en Spanje met een omvangrijke nationale defensie-industrie, kijkt de overheid over het algemeen eerst naar de eigen nationale industrie voor de aanschaf en de ontwikkeling van nieuwe producten. Voor kleine landen of leveranciers van niche-oplossingen is het nu nog lastig om een positie te verwerven in deze internationale supply chain.

Vraag en aanbod zijn niet transparant

Een belangrijke klacht van de aanbodzijde is dat de veiligheidsvraag onduidelijk is. In engere zin is dat voor de defensiebehoefte wel duidelijk. In een algemene COTS-setting, zowel voor Defensie als voor Maatschappelijke Veiligheid, is men sterk geneigd te kijken naar wat er beschikbaar is. Echter, ook het aanbod is niet erg transparant. Leveranciers bieden vaak producten aan die in algemene zin een vergelijkbare functionaliteit hebben, maar de preciese verschillen zijn onduidelijk. Vaak komt pas na de aanschaf en de implementatie de feitelijke functionaliteit naar voren. Voor het langere termijn onderzoek is onduidelijk hoe operationele behoeften zich vertalen naar een langere termijn

[27] Zie de rapporten van TNO (2006b) en het ministerie van Defensie en EZ (2007)

behoefte. Van de langere termijn R&D zijn de toepassingen niet altijd heel duidelijk en de termijn waarop de oplossingen beschikbaar komen. Dit is een karakteristiek die past bij de constatering dat Veiligheidsinnovatie nog relatief nieuw is en dat er nog relatief weinig samenhang en samenwerking is. Op onderdelen is dat er wel voor de vraag- en aanbodzijde; maar zeker nog niet voor een samenhang van én vraag én aanbod.

Veiligheidstechnologie bestaat niet

Een belangrijke constatering is dat veiligheidstechnologie als technologiegebied feitelijk niet bestaat, behalve voor een beperkt aantal onderwerpen zoals wapentechnologie. Er is vrijwel altijd sprake van bestaande 'enabling' technologie die ook kan worden toegepast voor veiligheid. Voorbeelden zijn sensoren, beeldverwerking, materialen, ICT etc. die breed toegepast kunnen worden voor milieu, duurzaamheid, medische systemen en ook voor veiligheid. Dit betekent dat er al veel interessant onderzoek wordt uitgevoerd zonder dat dit afhankelijk is van een directe aansturing of (substantiële) financiering vanuit een veiligheidsoptiek. Binnen deze bestaande onderzoeksgebieden is het veel meer de uitdaging om voldoende aandacht te vragen én te krijgen voor veiligheid als toepassing.
Bijvoorbeeld DNA wordt al heel lang onderzocht in kankeronderzoek, erfelijkheidsvraagstukken, ziekten etc. Het belang van DNA voor identificatie is van relatief recente datum. De belangstelling vanuit de veiligheidsoptiek heeft geresulteerd in een vraag naar en ontwikkeling van snellere en eenvoudigere DNA-meetsystemen. Dat was in de traditionele laboratoria-setting niet erg belangrijk.
Het is niet zinvol om een apart en specifiek een veiligheidsprogramma te definiëren, door de breedte van toepassingsgebieden voor deze technologievelden. Het is de uitdaging om bij de programmering binnen die technologiegebieden meer de aandacht te vestigen op de relevantie en de kansen op het gebied van Veiligheid. Alleen al het op de agenda krijgen dat veiligheid een toepassingsgebied kán zijn, is soms al voldoende voor veiligheidsgerichte oplossingen. Tot slot bestaat het gevaar dat kennis die op langere termijn nodig is om de Maatschappelijke Veiligheid te waarborgen, niet ontwikkeld wordt door het ontbreken van een gemeenschappelijk nationaal onderzoeksprogramma voor Veiligheid.

Er is weinig productie in Nederland

Nederland heeft slechts in beperkte mate productie in Nederland of vanuit Nederland aangestuurde productie. Voorbeelden van Nederlandse producten zijn Bosch camera's (voormalig Philips), GE Interlogix (beveiligingssystemen) of Boon Edam (draaideuren en toegangssystemen), Ten Cate en DSM (materialen). Voor een groot aantal softwaregebaseerde producten en diensten is er in Nederland wel sprake van 'productie' (softwareontwikkeling), maar dat is nog beperkt van schaal en vaak

ook nog niet uitontwikkeld.[28] In algemene zin is het positief als de gehele keten in een land aanwezig dus R&D én productie (of aangestuurde productie in het buitenland) én een voldoende grote (thuis)markt. Al eerder is geconstateerd dat de Nederlandse markt per definitie beperkt is qua omvang en dat een COTS-situatie wenselijk is. Als de productie buiten Nederland plaatsvindt of onvoldoende gebaseerd is op Nederlandse kennis en management, holt dat de basis voor R&D-capaciteit uit.

De afgelopen jaren is er een substantieel aantal grotere Nederlandse bedrijven overgenomen door internationale bedrijven op het gebied van veiligheid en innovatie, zoals Thales (onder meer voormalig Hollandse Signaal), Bosch (voormalig Philips), GE Interlogix (eerst zelfstandig) en binnenkort mogelijk Stork. De besluitvorming over de R&D verplaatst daarmee naar het buitenland. De kans is dan aanwezig dat R&D-activiteiten zich verplaatsen naar het buitenland. Voor deze verkenning is dit vraagstuk met een aantal van deze bedrijven besproken. Uit de gesprekken komt naar voren dat in de praktijk dit effect nog niet zichtbaar is. Een verklaring voor uitblijven van dit effect is de kracht van het 'human capital' die niet eenvoudig verplaatsbaar is (soms niet eens binnen Nederland). Buitenlandse overnames lijken voor de bestaande R&D geen probleem te zijn. Het is echter de vraag of de buitenlandse moeder voor nieuwe R&D-ontwikkelingen zal kiezen voor een ander land, in ieder geval niet in Nederland.

Wat bij een aantal overgenomen bedrijven een rol speelt is dat producten ontwikkelen die nog geen onderdeel uitmaakten van de buitenlandse moeder. Voorbeelden zijn bijvoorbeeld GE Interlogix of Bosch. De buitenlandse moederbedrijven hebben bij het onderkennen van Veiligheid als groeimarkt de overweging gemaakt om deze niet zelf op te zetten, maar te kiezen voor overname. Voor de overgenomen bedrijven geldt dat de buitenlandse moeder voor deze producten dan nog geen andere ontwikkelfaciliteit elders in de wereld heeft. Daarentegen zijn er wel voorbeelden van overnames waarvoor elders in de wereld wel vergelijkbare ontwikkelfaciliteiten worden opgezet. Daar is de beweging zichtbaar dat nieuwe onderzoeksactiviteiten wel degelijk naar de niet-Nederlandse dochters gaan. Dit onderbouwt de constatering dat een krachtige en goede kennisinfrastructuur, al dan niet in combinatie met kennisinstellingen, kan zorgen voor het niet makkelijk verplaatsbaar zijn van ontwikkelfaciliteiten en –activiteiten.

Tekort aan bèta's en technisch personeel

Diverse geïnterviewden constateerden een gebrek aan goed opgeleid technisch en bèta-personeel. Dit is een algemeen knelpunt en niet specifiek voor deze sector. Bedrijven die zich op de defensiemarkt richten mogen alleen personeel uit NAVO-landen aannemen waardoor we ook internationaal gezien op een krappere arbeidsmarkt zitten. Het onderwerp Veiligheid staat sterk in de

[28] RAND Europe (2004)

belangstelling en trekt het door programma's als Crime Scene Investigation veel aandacht. Er zijn verschillende nieuwe opleidingen van start gegaan, onder andere op het terrein van Forensic Science aan de Universiteit van Amsterdam.

Wet- en regelgeving sluiten niet altijd aan op technologische ontwikkelingen

Soms is wet- en regelgeving niet technologieneutraal en zijn nieuwe technologische oplossingen niet toegestaan. Een voorbeeld is dat de Lucht- en Verkeerswet nog niet voorziet in het gebruik van onbemande vliegtuigen voor bijvoorbeeld surveillance doeleinden. Testvluchten worden op dit moment alleen boven militair terrein gehouden. Een ander voorbeeld is dat nog bepaald moet worden of een wettelijke basis wenselijk is voor het al dan niet vastleggen van eisen aan toezichtruimte voor cameratoezicht.

Geen gestandaardiseerde producten

Een vorm van regulering die wat verder afstaat van de overheid is standaardisatie. Voor veiligheidsproducten zijn er nog weinig open standaarden. Er zijn wel zogenaamde 'mil-specs', dit zijn door de Amerikaanse defensie geformuleerde standaarden. Doordat de Amerikaanse markt zo groot en belangrijk is gelden deze de facto als standaard, zij het dat deze sterk eenzijdig geformuleerd is.

Voor meer commerciële producten en vooral ICT-gebaseerde diensten is het wenselijk dat er meer (open) standaarden komen voor interoperabiliteit en interconnectiviteit. Deze open standaarden maken het mogelijk dat softwaredeelsystemen van verschillende leveranciers aan elkaar gekoppeld worden en dat ook gewisseld kan worden van leverancier zonder vervanging van (deel)systemen. Ook voor leveranciers biedt dit mogelijkheden. Nieuwe deelsystemen zullen relatief eenvoudig te integreren zijn in combinatie met andere, bestaande, systemen. Een kanttekening is dat gestandaardiseerde oplossingen soms diametraal staan in veiligheidsvraagstukken. Bijvoorbeeld een stopknop of een noodknop die bij noodsituaties deuren ontsluit. Deze knop kan ook gebruikt worden voor bijvoorbeeld terroristische doeleinden (snel naar buiten kunnen, paniek zaaien).

Sociale, organisatorische en ethische factoren spelen een cruciale rol

Voor een succesvolle de operationele toepassing van innovatieve veiligheidsoplossingen spelen sociale, organisatorische en ethische onderwerpen een belangrijke rol. Voorbeelden zijn: onvoldoende getraind personeel of zelfs onkunde in het gebruik van geavanceerde communicatieapparatuur (met name in crisissituaties); verschil in de interpretatie van gegevens; en omgaan met informatie uit veel verschillende bronnen. Ook bij de validatie van simulaties (in hoeverre benader je de werkelijkheid), het integreren van verschillende nationale systemen, communicatie over veiligheid (laat weten wat je

allemaal doet zodat mensen zich veilig voelen), en innovatie van diensten spelen deze factoren een belangrijke rol.

Het ESRAB-rapport geeft een goed overzicht van deze factoren: het begrijpen van menselijk gedrag in crisissituaties en in normale situaties;

- profilering van terroristisch gedrag;
- de nationale systemen moeten interoperabel, schaalbaar en mobiel zijn;
- procedures en democratische controle van publieke services;
- toepassing van systemen in verschillende culturen;
- omgaan met onzekerheid;
- foresight;
- afwegingen tussen security en privacy en sociale cohesie;
- secure growth voor bedrijven (in lijn met green growth);
- prioriteiten stellen bij bedreigingen en onveilige gebieden net buiten de grenzen van Europa.

3 Kennis en innovatie

Dit hoofdstuk gaat in op kennis en innovatie rond Veiligheid. Allereerst worden de relevante nationale en internationale beleidsinitiatieven voor kennis en innovatie besproken. Vervolgens gaan we in op de inspanningen en prestaties van Nederlandse bedrijven en kennisinstellingen.

3.1 Nederlands innovatiebeleid en veiligheid

In Nederland is er een scala aan initiatieven en programma's rondom kennis en innovatie, die een relatie hebben met Veiligheid. Een overzicht van deze initiatieven (zowel lopende als de meest relevante afgeronde) wordt gegeven in de onderstaande tabel. Vervolgens worden deze initiatieven meer in detail besproken.

Tabel 8 *Overzicht nationale initiatieven en programma's*

Initiatief/programma	Looptijd
Sleutelgebiedenaanpak / Innovatieprogramma's ministerie van Economische Zaken	
- Point-One (nano-elektronica en embedded systems)	2006 – 2009
- High Tech Automotive Systems	2007 – 2010
- Materials to innovate the industry	2008 – 2011
Maatschappelijke innovatieagenda Veiligheid (Nederland Ondernemend Innovatieland)	2008 – 2011
Innovatiegerichte onderzoeksprogramma's (IOP's)	
- Beeldverwerking	1996 – 2007
- Self Healing Materials	2005 – 2012
- Photonic Devices	2006 – 2012
- Mens-Machine Interactie	1998 - 2010
Technologie & Samenleving (met deelprogramma Veiligheid)	1995 – 2002
Maatschappelijke Sectoren & ICT (met Veiligheid als een van de thema's)	2005 – 2008
Politie en Wetenschap	Sinds 1999
Sentinels	2003 – 2011
Veilig Verbonden	Vanaf 2007
Interactive Collaborative Information Systems (ICIS)	2004 – 2009
Technologie en Opsporing	Vanaf 2004
Nationaal Platform Criminaliteitsbeheersing (NPC)	Sinds 1992
CODEMA	Tot en met 2005
Actieplan Veilig Ondernemen (AVO) – deel 1 t/m 3	Sinds 2004
Veiligheid en Beeldverwerking	Vanaf 2008
Game Research for Training and Entertainment (GATE)	Vanaf 2007
Maritieme Veiligheid	Sinds 2004
Secure Haven	Vanaf 2007

Sleutelgebieden aanpak

Door het kabinet Balkenende II is het eerste Innovatieplatform ingesteld, met als doelstelling onder meer het versterken van de Nederlandse economie door het aanbrengen van focus in de inspanningen van overheden, kennisinstellingen en bedrijven op kansrijke gebieden. Het Innovatieplatform heeft zes sleutelgebieden aangewezen, te weten Flowers & Food, Hightech Systemen & Materialen, Water, Creatieve Industrie (allen in 2004), Chemie (2005) en Pensioenen en Sociale Verzekeringen (2006). Daarnaast heeft dit Innovatieplatform op het gebied van dienstverlening 'The Hague: Residence of Peace and Justice' aangewezen als opkomend sleutelgebied (in 2004). ICT en Energietransitie zijn bovendien erkend als innovatie-as voor alle sectoren van de economie (2005).[29]

Innovatieprogramma's van het ministerie van Economische Zaken

Het ministerie van Economische Zaken heeft de sleutelgebiedenaanpak overgenomen in haar programmatische aanpak voor innovatie: Innovatie in Dialoog.[30] Voor een aantal sleutelgebieden zijn inmiddels innovatiepro-gramma's ontwikkeld en gestart. Innovatieprogramma's worden ontwikkeld op terreinen waarin Nederland zich internationaal onderscheidt (excellentie), waar sprake is van voldoende economisch en maatschappelijk belang en waar sprake is van samenhang en (internationale) samenwerking (focus). Voor het onderwerp Veiligheid zijn de volgende innovatieprogramma's het meest relevant:

- Point-One[31], gericht op Nano-elektronica en Embedded Systemen.[32]
- High Tech Automotive Systems[33], dat zich met name richt op toeleveranciers in de automobielindustrie en waar 'driving safety' één van de aandachtspunten is.
- Materials to innovate the industry (M2i)[34], gericht op hightech materialen, waarbinnen ook aandacht zal zijn voor veiligheid.

Daarnaast is nog een aantal innovatieprogramma's in ontwikkeling die mogelijk raakvlakken met Veiligheid hebben, te weten: Diensteninnovatie en ICT en High Tech Systems (met mechatronica als zwaartepunt).

---

[29] Ministerie van EZ en SenterNovem (2007)
[30] Deze wordt uitgevoerd door SenterNovem. Voor meer informatie zie www.innovatieindialoog.nl
[31] www.pointone.nl
[32] In het kader van Point-One is het Cantate-RACE-project gefinancieerd dat zich richt op videobeeldanalyse. Dit project is het Nederlandse deel van het CANTATA project dat binnen het EUREKA cluster ITEA2 loopt.
[33] www.htas.nl
[34] www.m2i.nl; naar verwachting zal dit programma in 2008 officieel van start gaan.

Maatschappelijke innovatieagenda Veiligheid

In het beleidsprogramma 2007–2011 van het kabinet Balkenende IV 'Samen Werken, Samen Leven'[35] is als onderdeel van de pijler innovatie Veiligheid als maatschappelijk innovatiethema benoemd. Er is een interdepartementale programmadirectie Kennis en Innovatie in het leven geroepen[36] voor de uitvoering van het innovatiebeleid. Het opstellen van een langetermijnstrategie en concrete innovatieagenda's voor de maatschappelijke thema's als energie, water, zorg, onderwijs en veiligheid behoort tot de taken van de nieuwe programmadirectie.

De programmadirectie is onderverdeeld naar drie taakvelden, namelijk:

- het taakveld langetermijnstrategie;
- het taakveld maatschappij en innovatie;
- het taakveld versterken van innovatief vermogen.

De programmadirectie is van plan om binnen het tweede taakveld een analyse op het thema Veiligheid uit te voeren, met als doel om een maatschappelijke innovatieagenda Veiligheid op te stellen. Voor de jaren 2008–2012 is in totaal 54 miljoen euro beschikbaar voor de uitvoering van deze innovatieagenda. Dit rapport dient als input voor het uitvoeren van de analyse en het opstellen van de innovatieagenda. Ook het derde taakveld is van belang voor Veiligheid, omdat in dit taakveld onderwerpen als arbeidsmarkttekorten, valorisatie, SBIR[37] en launching customership worden opgepakt.

Innovatiegerichte onderzoeksprogramma's (IOP)

Het ministerie van Economische Zaken heeft ruim 25 jaar het IOP-instrument gehad, met als doel om het fundamenteel-strategisch onderzoek bij de publieke kennisinfrastructuur te versterken in een richting die aansluit bij de innovatiebehoeften van het bedrijfsleven. Een aantal afgeronde en lopende IOP's zijn relevant voor Veiligheid. Nog lopende IOP's zijn *Self Healing Materials*, *Photonic Devices* en *Mens-Machine Interactie.* Het IOP Self Healing Materials (2005-2012, circa tien miljoen euro) richt zich op zelf-herstellende structurele materialen: polymeren, metalen, civiele materialen en composieten & laminaten. Het onderzoek dient uiteindelijk te leiden tot een nieuwe klasse van betrouwbare en duurzame materialen. Het IOP Photonic Devices (2006-2012, circa elf miljoen euro) richt zich op twee thema's, namelijk ontwikkeling van geavanceerde lichtbronnen & detectiesystemen; en applicaties van photonic devices in 'health & medicine'. Het IOP Mens-Machine Interactie (1998-2006) is gericht op ontwerp, implementatie en evaluatie van 'intelligente systemen'. Deze focus past in het bredere onderwerp 'Ambient Intelligence'. Het onderzoekspro-

[35] Nederland (2007)
[36] Voor meer informatie zie www.kennis-innovatie.nl
[37] http://www.senternovem.nl/sbir/

gramma is beperkt tot multi-user toepassingen, ofwel mens-mens interactie ondersteund door een intelligent systeem, of meerdere gebruikers die interacteren met een dergelijk systeem. Een afgerond IOP die relevant is voor Veiligheid is *Beeldverwerking*. Het IOP Beeldverwerking (1996-2007) richtte zich op het gebruik van beeldverwerking of vision, dat steeds meer toeneemt. Apparatuur is meer en meer voorzien van zelfsturende en waarnemende functies via mechanisatie en sturing met elektronica. Naast toepassingen in de zorg is ook veiligheid een maatschappelijk domein waar beeldverwerking een belangrijke rol speelt. Zo is een compleet veiligheidssysteem voor op en rond het voetbalstadion van ADO Den Haag ontwikkeld.[38]

Maatschappelijke veiligheid

Over maatschappelijke veiligheid had de overheid geen duidelijk innovatiebeleid. In de jaren tachtig was er het Landelijk Bureau Voorkoming Misdrijven (LBVM) dat primair gericht was op preventie met een breed scala aan maatregelen en technische voorzieningen. In de periode 1995-2002 was er het interdepartementale stimuleringsprogramma 'Technologie & Samenleving' (T&S), met het deelprogramma Veiligheid.[39] De basis voor dit pro-gramma was de beleidsnota 'Kennis in beweging' dat als achtergrond had dat innovatie kon bijdra-gen aan het oplossen van maatschappelijke vraagstukken.[40] Uit de evaluatie van dit programma komt naar voren dat het T&S-netwerk dat zich rond de projecten van innovatoren ontwikkelde als een succes werd ervaren.

Maatschappelijke Sectoren & ICT

Sinds 2006 is er het interdepartementale actieprogramma 'Maatschappelijke Sectoren & ICT', waar-binnen veiligheid één van de vier thema's is.[41] Het programma richt zich op de opschaling van succesvolle, maar nog kleine en lokale toepassingen van ICT. Voor dit actieprogramma is een budget beschikbaar van veertig miljoen eurovoor de periode 2005-2008. Het programma is gefinancierd vanuit het Fonds Economische Structuurversterkingen (FES).[42] Tot nu toe is alleen in de eerste prijsvraag een veiligheidsproject gehonoreerd.[43] Voor de vijfde prijsvraag is 'Serious Gaming en Simulatie voor een betere Veiligheid' als thema benoemd. Eén van de constateringen is dat het moeilijk is om ICT-projecten te 'vinden' die op lokale schaal al operationeel zijn en die 'klaar' zijn om opgeschaald te worden. Mogelijk is de vorm een andere verklaring aangezien de prijsvraag als complex en ingewikkeld ervaren wordt.

---

[38] http://www.senternovem.nl/iop_beeldverwerking/index.asp
[39] CCV (2005)
[40] Ministerie van EZ (1995)
[41] www.m-ict.nl
[42] zie bijvoorbeeld AWT (2007)
[43] Project Utrecht

Politie en Wetenschap

Binnen de politieorganisatie krijgt innovatie veel aandacht, vooral het verbeteren van de ICT-toepassingen binnen de politieorganisatie en de communicatie met haar partners, zoals C2000.[44] Ook heeft de politie een Innovation Board, dat sinds 2006 wordt aangestuurd vanuit de Raad van Hoofdcommissarissen (RvHC). Sinds 1994 wordt jaarlijks de Politie Innovatieprijs (PIP) uitgereikt. Verder is er sinds 1999 het programma 'Politie en Wetenschap'.[45] Het onderzoeksprogramma Politie en Wetenschap is een onderdeel van het Kennisnetwerk van de Politieacademie. De kernactiviteit is het programmeren en uitvoeren van het meerjarenonderzoeksprogramma, gerelateerd aan de ontwikkeling en uitvoering van beleid op het gebied van de veiligheid in de Nederlandse samenleving.

Sentinels

Sentinels is het Nederlandse onderzoeksprogramma op het gebied van informatiebeveiliging, beveiliging van informatiesystemen en van computernetwerken.[46] Dit programma wordt gefinancierd vanuit het technologiefonds van de Stichting Toegepaste Wetenschap (STW) en het FES. Binnen het Sentinelsprogramma worden een tiental projecten uitgevoerd met een gezamenlijk budget van bijna zes miljoen euro.

Veilig Verbonden

Voortbouwend op Sentinels is het onderzoeksprogramma 'Veilig Verbonden' geformuleerd.[47] In mei 2007 verscheen vanuit ICTRegie een rapport waarin de onderzoeksagenda is geschetst die nodig is om de veiligheid van ICT-netwerken te optimaliseren, aangezien deze ICT-infrastructuur essentieel is als key enabler voor de Nederlandse economie. ICTRegie heeft in dit kader het ICT-Innovatieplatform (IIP) Veilig Verbonden opgericht.[48] Dit IIP is voorgekomen uit het NVSO (Nationaal Samenwerkingsverband Security Onderzoek).[49]

Interactive Collaborative Information Systems (ICIS)

Binnen de BSIK-regeling (Besluit Subsidies Investeringen Kennisinfrastructuur) is het project ICIS gehonoreerd. Dit project wordt uitgevoerd door het DECIS-lab, een open consortium opgericht door

---

[44] Politie Nederland (2006)
[45] www.politieenwetenschap.nl
[46] www.sentinels.nl
[47] ICTRegie (2007)
[48] http://www.ictregie.nl/iip/index.php?pageId=34
[49] Het NVSO is een samenwerkingsverband tussen bedrijven, onderzoeksinstellingen, marktpartijen, en eindgebruikersorganisaties, zoals CTIT, TNO, Philips Research, TU/e, KUN, TNT Post, KPN, Dartagnan/Schiphol, Chess, Irdeto Access, Nederlandse Vereniging van Banken, ministerie van EZ, NicTiz.

Thales Nederland, TU Delft, Universiteit van Amsterdam en TNO.[50] Het idee achter ICIS is om uiterst complexe informatiesystemen intelligenter en effectiever te maken voor besluitvormingsprocessen. Hierbij moet gedacht worden aan intelligente systemen om relevanties uit die data te halen, patronen te herkennen en managementinformatie te destilleren. Veiligheid is een belangrijk toepassingsgebied van dit onderzoek. Ook het BSIK-programma is vanuit het FES gefinancierd.

Technologie en Opsporing

In 2005 heeft de Commissie Winsemius haar advies uitgebracht.[51] In dit advies lag het accent op de kansen die technologie biedt voor nieuwe oplossingen, maar ook voor de bedreigingen van nieuwe vormen van criminaliteit. In zijn reactie op het advies aan de Tweede Kamer heeft de minister van Justitie aangegeven een platform Technologie en Opsporing in te zullen stellen. Dat platform is geïnstalleerd, maar is niet erg actief. Mogelijk dat het platform in het nieuw op te stellen innovatieprogramma opnieuw opgepakt kan worden. Het platform past in die zin in het subthema 'opsporing' van het R&D-programma Maatschappelijke Veiligheid (RDMV) van BZK.

Nationaal Platform Criminaliteitsbeheersing (NPC)

Het Nationaal Platform Criminaliteitsbeheersing (NPC) is een in 1992 opgericht samenwerkingsverband tussen overheid en bedrijfsleven gericht op het aanpakken van criminaliteit waar het bedrijfsleven slachtoffer van wordt. Het NPC is samengesteld uit een gelijk aantal vertegenwoordigers van overheid en bedrijfsleven. Alle relevante departementen, de politie, het openbaar ministerie en de VNG zijn in het platform vertegenwoordigd. Namens het bedrijfsleven maken werkgeversorganisaties deel uit van het platform. Ook is een groot aantal branches vertegenwoordigd.

CODEMA

De Nederlandse defensie-industrie heeft een heel behoorlijke innovatietraditie. Qua omvang is deze weliswaar niet vergelijkbaar met de grote landen als de Verenigde Staten, het Verenigd Koninkrijk, Frankrijk, Duitsland of Spanje. Nederland is binnen Europa wel de grootste van de kleine landen, achter het Verenigd Koninkrijk, Spanje, Frankrijk, Duitsland en Zweden. Een goed voorbeeld is Nederlandse positie op het gebied van fregatten met de Goalkeeper. Vanaf de jaren '70 tot 2004 was het CODEMA-programma actief dat geresulteerd heeft in een groot aantal innovaties, zoals MUNOS nachtzichtkijkers, de ALBOTROSS hoge resolutie warmtebeeldsensor en de SMART-L langeafstands 3-D radar. In 2005 is het CODEMA-programma beëindigd. Er is op het moment geen

[50] http://www.decis.nl/content/view/40/28/
[51] Winsemius (2005)

ander innovatiestimuleringsinstrument op het gebied van defensie bij EZ. Vanuit de sector wordt ervoor gepleit een met CODEMA vergelijkbaar programma op te zetten.[52]
Wel is er een uitgebreid R&D-instrumentarium bij Defensie zelf aanwezig. Defensie voert momenteel het project Verbeterd Operationeel Soldaat Systeem (VOSS) uit, dat onderdeel is van het Soldier Modernisation Programma (SMP) dat voorziet in een aantal verbeteringen van de uitrusting van de te voet optredende soldaat.[53] VOSS past in het streven om te voorzien in betere bescherming van ingezette eenheden en het vermogen op te treden in netwerken (Network Enabled Capabilities) verder te vergroten.

Actieplan Veilig Ondernemen (AVO)
De samenwerking tussen overheid en bedrijfsleven wordt geconcretiseerd in de Actieplannen Veilig Ondernemen (AVO). In juli 2007 is het AVO deel 3 gepresenteerd met als doel de criminaliteit met 25% terugdringen in 2010, gemeten ten opzichte van begin 2004.[54] Het beleid van het NPC en ook het AVO 3 richten zich vooral op de aanpak van concrete en urgente criminaliteitsvraagstukken. Er is geen sprake van een onderzoekscomponent.

Veiligheid en Beeldverwerking
Vanuit het IOP Beeldverwerking[55] (afgerond eind 2007) en het daaraan gelieerde MultiMediaN programma[56] is het initiatief opgepakt om in 2008 een community rond Veiligheid en Beeldverwerking op te starten.[57] Het initiatief richt zich op het voortbrengen van een nieuwe generatie intelligente camera surveillance systemen die in hoge mate geautomatiseerd zijn.

GATE
Het GATE-programma wordt uitgevoerd door een consortium van acht partners: Universiteit Utrecht (penvoerder), TNO, Hogeschool voor de Kunsten Utrecht, Universiteit Twente, Technische Universiteit Delft, Nederland Breedbandland, Waag Society en Thales, gesteund door ICTRegie. Behalve deze acht partners zullen MKB-bedrijven participeren. Het kabinet stelt tien miljoen euro beschikbaar, bovenop de negen miljoen euro eigen inbreng van de deelnemende instellingen. De creatieve industrie is één van de sleutelgebieden voor de Nederlandse economie. Een sterk groeiende component daarbinnen is gaming. Gaming gaat veel verder dan computergames. Er bestaat een grote

[52] zie http://www.niid.nl/article.aspx?i=204
[53] zie http://www.mindef.nl/materieelprojecten/landstrijdkrachten/overzicht/
[54] Nationaal Platform Criminaliteitsbeheersing (2007)
[55] www.senternovem.nl/iop_beeldverwerking
[56] www.multimedian.nl
[57] Bron: SenterNovem (ir. H. Teunissen)

markt van gaming- en simulatietoepassingen in maatschappelijke en economische sectoren als gezondheidszorg, onderwijs, mobiliteit, veiligheid en openbare dienstverlening.[58]

Maritieme veiligheid

Door de aanslag op de Twin Towers van 9/11 zijn er strengere eisen geformuleerd voor de veiligheid van havens. Deze eisen zijn geformuleerd door de International Maritime Organization (IMO)[59] en zijn bekrachtigd in een richtlijn van de Europese Commissie. In Nederland is dit vertaald in de Havenbeveiligingswet van 2004.[60] Op basis van deze wet en achterliggende regelgeving moeten havens een havenveiligheidsplan hebben en ook uitvoering geven aan concrete veiligheidsmaatregelen. Inmiddels voldoen de grote Nederlandse zeehavens aan dit veiligheidsbeleid. In de nabije toekomst moeten ook laad- en losplaatsen aan binnenwateren voldoen aan de veiligheidsrichtlijnen.
Dit veiligheidsbeleid heeft, op dit moment, nog geen specifieke innovatieve doelstelling. Wel is de havenveiligheid en grenscontrole een belangrijk onderwerp in het zevende Kaderprogramma (KP7). De Rotterdamse haven participeert wel, zij het beperkt, in één van de recente KP7-projecten. Het belang van transport en logistiek voor de Nederlandse economie en de vooraanstaande positie van de Rotterdamse haven in relatie met de kwetsbaarheid van vitale infrastructuren zou een goede basis kunnen zijn voor innovatief onderzoek. Havenveiligheid past in een breder perspectief van mainport security dat ook betrekking heeft op luchthavens en met name Schiphol.

Secure Haven

Met Den Haag als kern is er een initiatief om te komen tot een 'Secure Haven'.[61] Hierbij gaat het niet alleen om het versterken van de internationale positie van Nederland op het gebied van internationaal strafrecht, maar ook om technologische aspecten: Het concept Secure Haven beoogt de bescherming van kwetsbare gebieden zodanig vorm te geven dat veiligheidsmaatregelen onopgemerkt blijven. Uitgangspunt van het concept is de verbinding tussen veiligheid en kwaliteit van leven, gekoppeld aan professionele activiteiten. Bij technologische oplossingen voor de beveiliging van kwetsbare gebieden, een aantrekkelijke inrichting van ruimte, hoogwaardige infrastructuur en dienstverlening en door ook de juridische aspecten van beveiliging niet uit het oog te verliezen worden deze doelen nagestreefd. Dit programma valt onder het opkomende sleutelgebied 'The Hague: Residence of Peace and Justice'.[62]

---

[58] http://62.148.175.94/pona/bekijkpers.cfm?style=standaard&persberichtid=816
[59] Internationale Ship and Port Security Code (ISPC)
[60] http://www.eerstekamer.nl/9324000/1f/j9vvgh5ihkk7kof/vgqvhea1d06h
[61] Campus Den Haag en Universiteit Leiden (2007)
[62] Ministerie van EZ en SenterNovem (2007)

3.2 Internationaal veiligheidsbeleid en veiligheidsonderzoek

De nadruk van deze verkenning ligt op de Europese regelgeving en beleidscoördinatie en op het Europese R&D-programma veiligheid/KP7. Er wordt niet ingegaan op het Europese 'buitenlandse' veiligheidsbeleid of op de Europese participatie in NAVO- en/of andere internationale operaties. Veiligheid (security) is één van de tien thematische beleidsprioriteiten van KP7. Na een toelichting van het Europese veiligheidsbeleid en veiligheidsonderzoek, presenteren we op hoofdlijnen het nationale beleid en onderzoek van enkele Europese landen.

European Security Research Programme (ESRP)

Het Europese onderzoeksbeleid op het gebied van veiligheid vindt, net als het Nederlandse, zijn oorsprong in de 9/11-aanslag in New York, de aanslag in Madrid en de daaruit voortvloeiende aandacht voor terroristische aanslagen en veiligheid in het algemeen. De basis voor een Europees onderzoeksbeleid was het advies 'Research for a secure Europe' uit 2004 onder leiding van de toenmalige EU-commissarissen Busquin en Liikanen.[63] Eén van de aanbevelingen was om een European Security Research Programme te formuleren dat in 2007 zou moeten starten. Als voorbereiding op dit ESRP heeft de Europese Commissie voor 2004-2006 een Prepatory Action Security Research (PASR) uitgevoerd.[64] Dit PASR-programma had een beperkt budget van ongeveer vijftien miljoen euro per jaar. Binnen dit budget konden er daardoor tien tot twintig projecten per jaar gehonoreerd worden, terwijl er jaarlijks bijna 200 projectvoorstellen werden ingediend. Ondanks de beperkte omvang participeerden meer dan vijftig Nederlandse onderzoeksinstellingen en bedrijven in PASR (zie bijlage 4). Nederland stond hiermee op de zesde positie. In 2007 heeft het ESRP vorm gekregen als onderdeel van KP7. Uit de eerste ESRP-indieningsperiode komt naar voren dat Nederland in dertien projecten participeert (zie bijlage 5). Dit is een aandeel van 3,8% (hetgeen iets minder is dan het gemiddelde Nederlandse aandeel). In september 2007 is er een publiek private dialoog gestart in het European Security Research and Innovation Forum (ESRIF) overleg, wat eind 2009 zal leiden tot een Gemeenschappelijke Veiligheids Onderzoeksagenda. Deze agenda zal de basis vormen voor het werkprogramma Security in KP7. Het ESRIF zal het werk voortzetten dat door de European Security Research Advisory Board (ESRAB) en de Group of Personalities is opgeleverd. Eind 2007 zal het ESRIF volledig operationeel zijn. Het forum heeft een tijdelijk karakter waarbij het eind 2009 ontbonden zal worden.[65]

---

[63] Europese Commissie (2004b)
[64] Europese Commissie (2004)
[65] www.senternovem.nl/egl/nieuws/index.asp (04-10-2007)

Naast het ESRP dat specifiek is gericht op R&D kent de Europese Commissie nog een aantal andere stimuleringsprogramma's voor veiligheid. Hoewel deze programma's niet specifiek gericht zijn op innovatie is er veelal een technologiecomponent en is er daarnaast veel aandacht voor inter-Europese uitwisseling van gegevens en koppeling van systemen. In deze programma's is er verder veel aandacht voor operationele samenwerking van veiligheidsdiensten waarbij training en opleiding belangrijke elementen vormen. Deze elementen sluiten aan op innovatieve ontwikkelingen op het gebied van command & control, simulatie, serious gaming, etc. Deze Europese stimuleringsprogramma's zijn onder meer:[66]

- *Prevention of and fight against crime*
  Dit programma, met een budget van 597,6 miljoen euro voor de periode 2007-2013, richt zich op het verhogen van het niveau van veiligheid door het verkomen en bestrijden van al dan niet georganiseerde criminaliteit (met name terrorisme, mensenhandel, misdrijven tegen kinderen, illegale drugshandel en illegale wapenhandel, corruptie en fraude).
- *Prevention, preparedness against terrorism and other crime*
  Het programma heeft een budget van 137,4 miljoen euro voor de periode 2007-2013. Het programma ondersteunt de inspanningen van de lidstaten om terroristische aanslagen en andere veiligheidsincidenten te voorkomen, zich hierop voor te bereiden en mensen en kritieke infrastructuur hiertegen te beschermen. Daarnaast heeft het programma tot doel bij te dragen aan onder andere crisisbeheersing, milieu, volksgezondheid in terrorisme en andere aan veiligheid gerelateerde risico's binnen de ruimte van vrijheid, veiligheid en recht.
- *Criminal Justice*
  Het programma Criminal Justice heeft voor 2008 een budget toegekend gekregen van 29,8 miljoen euro. Het totale budget van 2007-2013 bedraagt 199 miljoen euro. [67]Het programma heeft onder andere als doel het bevorderen van de justitiële samenwerking om bij te dragen aan de totstandkoming van een Europese rechtsruimte in strafzaken.
- *Civil Protection Financial instrument*
  Het financieringsinstrument voor civiele bescherming kent een budget van 17,9 miljoen euro voor 2008 en is gericht op het ondersteunen en aanvullen van de lidstaten in geval van natuur- of door de mens veroorzaakte rampen, daden van terrorisme of technologische, radiologische of milieuongevallen.

[66] zie http://www.2007-2013.eu/by_scope_security.php
[67] zie http://www.2007-2013.eu/by_scope_criminal_justice.php

Veiligheidsonderzoek en innovatie in andere landen

Aansluitend bij dit Europese veiligheidsbeleid wordt een overzicht gegeven van veiligheidsonderzoeksprogramma in een aantal Europese landen. Voor een deel zijn deze nationale programma's bedoeld als complementair aan het ESRP. Hieronder wordt een korte beschrijving gegeven van de onderzoeksprogramma's uit Finland, Duitsland, Zweden, Oostenrijk, Verenigd Koninkrijk en Frankrijk. In bijlage 3 is een uitgebreide beschrijving opgenomen.

- *Finland*

  In Finland is de overheid via Tekes deze zomer een technologieprogramma gestart en een call geopend op het gebied van Safety en security (hier valt bijvoorbeeld ook voedselveiligheid onder). De Finse overheid ziet een belangrijke internationale markt, waar het land door haar goede kennispositie en beschikbare technologieën een rol kan spelen. De drijfveer lijkt hier, in tegenstelling tot andere landen, veel minder de nationale veiligheid te zijn. Het programma loopt tot 2012 met een totaal overheidsbudget van 80 miljoen euro, de deelnemende bedrijven en kennisinstellingen dragen aanvullend ook 80 miljoen euro bij. Voorlopig richt het programma zich op ontwikkeling van systemen die worden gebruikt in crisissituaties en safety en security technologie gerelateerd aan mobiliteit van goederen en mensen. Andere aandachtspunten zijn methoden voor risk assessment en de ontwikkeling van businessmodellen voor de safety en security sector.

- *Duitsland*

  Dit jaar presenteerde Duitsland zijn veiligheidsprogramma met de titel "Forschung für die zivile Sicherheit – Programm der Bundesregiering". [68]Het programma loopt in elk geval voor een eerste periode van 2007 tot 2010 met een budget van 123 miljoen euro. Het programma richt zich op scenariogericht veiligheidsonderzoek en op technologieën. Voor de technologieën ligt de nadruk vooral op de terreinen van een geïntegreerd beschermingssysteem voor hulpdiensten, multi-sensorsystemen voor gevaarlijke stoffen, patroonherkenning en biometrie. In Duitsland loopt naast dit programma een apart programma (sinds 2003) op het gebied van ICT-veiligheid.

- *Zweden*

  VINNOVA schreef in 2004 een advies op het gebied van security R&D, waarin zij de volgende veiligheidsclusters benoemden: complex systems and simulation; IT security; sensor technology; mobile solutions; physical transportation; NBC (nuclear, biological,

chemical); weapon technology.[69] Zweden heeft inmiddels een programma op het gebied van security. Het programma loopt in de periode 2007-2009. Het programmadoel is om in 2010 het Zweedse onderzoek en de industrie te benutten, zodanig dat ze significant bijdragen aan een verhoogde veiligheid in Zweden en de wereld. Het onderzoeksprogramma heeft de volgende (sub)doelen:

- Eenvoudiger maken voor Zweedse onderzoeksgroepen om deel te nemen in Europese onderzoeksprogramma's;
- Faciliteren van deelname in Amerikaanse security onderzoeksprogramma's;
- Innovatiecapaciteit voor de industrie creëren;
- Ontwikkelen van technologie en diensten die uiterlijk in 2010 gedemonstreerd kunnen worden.

- *Oostenrijk*

In Oostenrijk heeft men een nationaal onderzoeksprogramma op het gebied van veiligheid. Het programma is gericht op een samenspel van technologisch, sociaal en geesteswetenschappelijk onderzoek. Er is een budget beschikbaar van 110 miljoen euro in de periode 2005-2013. Er zijn vier programmalijnen:

- Netwerken en verkenningen;
- Gemeenschappelijke R&D-projecten;
- Gemeenschappelijke componentenontwikkeling en demoprojecten;
- Flankerende activiteiten.

Inhoudelijk richt het programma zich in de eerste fase alleen op bescherming van de kritische infrastructuur, waarbij naast het voorkomen van materiële schade ook het voorkomen van sociaal-psychologische schade centraal staat. Het is niet bekend op welke specifieke onderwerpen het programma zich de komende jaren gaat richten.

- *Verenigd Koninkrijk*

De Home Office heeft een "Science and Innovation Strategy"opgesteld voor de periode 2005-2008. De overheid investeert jaarlijks 60 miljoen pond. Voor de komende vijf jaar zijn negen prioriteiten aangemerkt, waaronder: minder misdaad; georganiseerde misdaad stoppen; terrorisme; en meer misdadigers voor het gerecht. In de toekomst verwacht men de volgende technologieën het meest nodig te hebben: identificatie; politiewetenschap en –

[68] Federal Ministry of Education and Research (2007)
[69] Vinnova (2005)

technologie (waaronder DNA-analyses, lab-on-a-chip, imaging); tracking technologie (onder andere RFID).

- *Frankrijk*

  De Franse infrastructuur kenmerkt zich door een groot aantal kerncentrales en een sterk ontwikkelde transportinfrastructuur. De technologievelden die daarom in Frankrijk onder de aandacht staan zijn toegangscontrolesystemen en observatiesystemen voor evenementen en vitale infrastructuur. Via het Agence Nationale de la Recherche (ANR) heeft de Franse overheid in 2006 een aanbesteding uitgeschreven om projectmatig onderzoek op het gebied van veiligheid te stimuleren. Voorbeelden van projecten zijn: veiligheid op de Middellandse Zee, defensietechnologie voor burgerveiligheid en EuroCop (efficiëntie van de politie te voet). Frankrijk heeft daarnaast een R&D-programma om detectietechnieken tegen bioterrorisme te ontwikkelen en is in de gemeente Elancourt een proeftuin gestart voor nieuwe veiligheidssystemen. Verder houden verschillende Franse technologieclusters (Pôles de Compétitivité) zich bezig met veiligheid. Zo is er een Pôle voor de beveiliging van communicatiesystemen, een Pôle voor de verhoging van veiligheid in havens en op zee, een Pôle voor natuurrampenbestrijding, één voor de strijd tegen bioterrorisme en één voor intelligente en proactieve technologie ter beveiliging van openbare ruimten en vitale infrastructuur.

3.3 Inspanningen en prestaties Nederlandse bedrijven en kennisinstellingen

In hoofdstuk 2 is een beeld geschetst van de veiligheidssector. In deze paragraaf komen de inspanningen en prestaties van deze sector voor kennis en innovatie aan de orde. Eerst schetsen we een beeld van de Nederlandse R&D-inspanningen op het gebied van veiligheid. Aansluitend gaan we in op de participatie in Europese projecten, internationale publicaties en octrooien. We sluiten het hoofdstuk af met de impressie van buitenlandse experts.

R&D-inspanningen Nederlandse bedrijfsleven

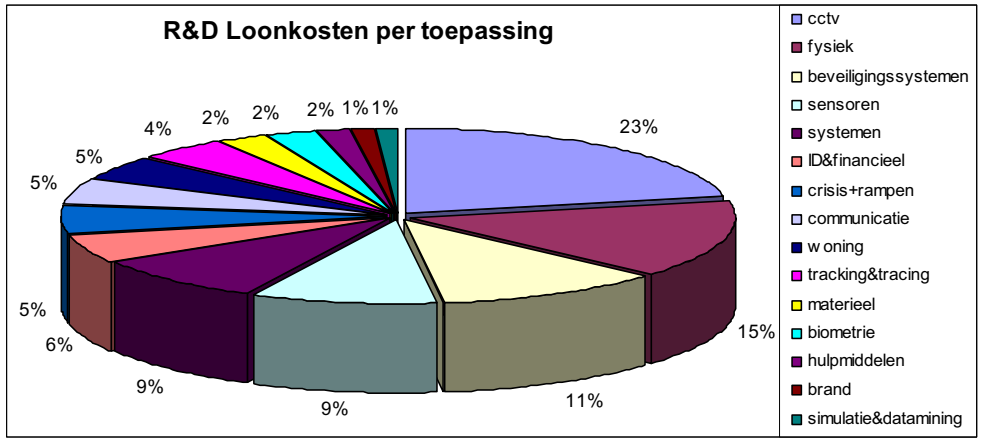
Om een beeld te schetsen van de R&D-inspanningen van het Nederlandse bedrijfsleven op het gebied van veiligheid, bieden twee studies van SenterNovem naar respectievelijk de defensiegerelateerde industrie en de security industrie inzicht.[70] De belangrijkste uitkomsten van deze studies zijn gebaseerd op de relevante projecten die zijn gehonoreerd volgens de Wet Bevordering Speur- en Ontwikkelingswerk (WBSO)[71] (in bijlage 7 zijn de belangrijkste cijfers opgenomen en worden deze

[70] SenterNovem (2004) resp. SenterNovem (2007)
[71] De WBSO is een fiscale stimuleringsregeling voor speur- en ontwikkelingswerk. Zie www.senternovem.nl/wbso

toegelicht). De studie naar de R&D-inspanningen van de defensiegerelateerde industrie gaat over de periode 2001-2003 en de studie naar de veiligheidsindustrie behandelt de periode 2003-2005.[72] Al zijn de beide perioden niet gelijk en is het moeilijk om over een periode van drie jaar uitspraken over trends te doen, toch komt in beide onderzochte perioden voor de twee industrieën een redelijk stabiel beeld van de R&D-inspanningen naar voren. Belangrijk is dat in beide studies alleen projecten zijn meegenomen waarbij in de projectomschrijving expliciet of duidelijk herken-baar gesproken wordt van een defensiegerelateerde, of een veiligheidsgerelateerde toepassing. Beide studies schetsen daardoor een ondergrens van de R&D-inspanningen.

De ondergrens van de R&D-loonkosten van de veiligheidsindustrie ligt aanzienlijk lager dan die van de defensiegerelateerde industrie, gemiddeld tien miljoen euro per jaar versus gemiddeld veertig miljoen euro per jaar. Wanneer deze bedragen worden afgezet tegen de jaarlijkse totale R&D-loonkosten in de WBSO (2,1 miljard euro in 2005) betekent dit dat de deze ondergrenzen duiden op een aandeel van respectievelijk 0,5% en 1,9% van de totale R&D-omvang.[73]

Figuur 2 *Verdeling van R&D-loonkosten van veiligheidsindustrie naar toepassing (bron: SenterNovem, 2007)*



In Figuur 2 zijn de R&D-loonkosten van de veiligheidsindustrie ingedeeld naar toepassing. Het blijkt dat bijna een kwart van de R&D-loonkosten binnen veiligheid wordt besteed aan onderzoek naar de toepassing camerasystemen. Op de tweede plaats volgt de toepassing die ligt in de sfeer van

[72] In de studie naar veiligheid zijn defensiegerelateerde projecten buiten beschouwing gelaten
[73] ter vergelijking: de chemische industrie omvat ruim 10% van de WBSO, high tech materialen ongeveer 5% en de scheepsbouwindustrie ongeveer 1% (bron: SenterNovem, 2006/2007b/2007c).

fysieke (object-)beveiliging, zoals toegangsdeuren. En op de derde plaats de beveiligingssystemen. Met deze categorie wordt niet-fysieke (object-)beveiliging bedoeld. Het gaat dan om beveiligingssystemen die betrekking hebben op ondernemingen en instellingen, zoals professionele alarm- en bewakingssystemen. De categorie woning is hieraan gerelateerd, al is deze gericht op particulieren. De vierde categorie sensoren betreft niet alleen de R&D voor individuele sensoren, maar ook het (detectie-)systeem waar ze onderdeel van uitmaken. De detectie van personen maakt in verschillende vormen deel uit van diverse andere categorieën, zoals biometrie, Closed Circuit Television (CCTV), beveiligingssystemen en tracking & tracing. De meer traditionele materialen voor in hoofdzaak bestrijding en anderzijds relatief nieuwe, vaak op preventie gerichte, technologieën als biometrie, tracking & tracing en simulatie/datamining hebben een bescheiden omvang aan R&D-loonkosten. Waar sensoren binnen veiligheid op een vierde plaats eindigt, blijkt uit de studie naar de defensiegerelateerde industrie dat 42% van de R&D-inspanningen hierop gericht is. Hier zijn echter ook de R&D-loonkosten van onderzoek naar radar en sonar toe gerekend. Onderzoek naar de toepassing command & controlsystemen neemt een tweede plaats in binnen het defensie onderzoek.

Uit de studies blijkt verder dat binnen de veiligheidsindustrie de technologieën communicatie en elektrotechniek bijna tweederde van de loonkosten voor hun rekening nemen. De technologieën regel- en computertechniek en werktuigbouwkunde (mechanica) volgen met respectievelijk 10% en 7%. De studie naar de defensiegerelateerde industrie laat een vergelijkbaar beeld zien. Ook zijn ICT (communicatie en regel- en computertechniek samengevoegd) en elektrotechniek de technologieën waar de nadruk op ligt. Mechanica volgt op een derde plaats. Onderzoek gericht op materiaaltechnologie binnen de defensiegerelateerde industrie heeft betrekking op circa 8% van de R&D-loonkosten, terwijl in de studie naar de veiligheidsindustrie deze technologie niet naar voren komt. Dit is opvallend, aangezien deze technologie ook nadrukkelijk wordt aangewend voor de ontwikkeling van bijvoorbeeld brand-, steek- en kogelwerende kleding voor politie en brandweer.

Participatie in Europese projecten

Voor een deel vinden de Nederlandse R&D-inspanningen ook plaats binnen Europese programma's. Binnen KP6 zijn zestien aan veiligheid gerelateerde projecten gevonden waarin Nederlandse organisaties participeerden. De subsidiebijdrage aan Nederlandse spelers in deze projecten bedroeg in totaal 4,5 miljoen euro.[74] In bijlage 5 zijn de relevante projecten en hun Nederlandse deelnemers binnen KP6 opgenomen. Nederlandse bedrijven voerden ook R&D-projecten uit in het Prepatory Action Security Research (PASR), dat de voorloper was van het Security thema in KP7.

[74] SenterNovem (2007)

Nederlandse organisaties kregen in de periode 2004-2006 ook via PASR 4,5 miljoen euro aan subsidie (als volgt verdeeld over de jaren: 1,8 miljoen euro, 2,2 miljoen euro en 0,5 miljoen euro). Hiermee was Nederland nummer zes in Europa. Begin 2007 is KP7 gestart met als tiende onderdeel het ESRP. Nederlandse organisaties kregen in de eerste indieningsronde voor ruim 5 miljoen euro aan subsidie toegewezen.

Internationale publicaties

Door het informatiecentrum van EZ is een onderzoek uitgevoerd naar peer-reviewed artikelen.[75] De studie wijst op 63 onderzoeken op het gebied van veiligheid. Van het onderzoek van de Vrije Universiteit Amsterdam valt op dat er aan deze universiteit veel onderzoek in opdracht van de Europese Unie wordt gedaan. In de periode van 2005-2007 zijn 53 publicaties bekend. Uit het onderzoek naar de mate waarin deze publicaties zijn geciteerd op Google Scholar en Scopus blijkt dat vooral de publicaties van de universiteiten van Amsterdam en de Universiteit van Tilburg veel geciteerd worden, hetgeen een indicatie is voor een hoge kwaliteit van onderzoek.

Octrooien

Op verzoek van de projectgroep heeft het Octrooicentrum Nederland gekeken naar de octrooien op het gebied van veiligheid. Voor deze verkenning zijn alleen octrooien die een directe veiligheids-toepassing hebben meegenomen in het onderzoek. De gevonden octrooien zijn gegroepeerd rond zes technologische thema's. Het gaat om de thema's: Materialen, Beeldverwerking, Elektrotechniek, Computers, Sensoren en ICT. In bijlage 6 worden de uitkomsten van het octrooionderzoek uitgebreid besproken. Hieronder gaan we in op enkele opvallende uitkomsten. Allereerst blijkt dat Nederland het qua octrooipositie niet slecht doet op het gebied van veiligheid in vergelijking met andere landen. De grote landen Amerika, het Verenigd Koninkrijk, Duitsland en Frankrijk hebben weliswaar (veel) meer octrooien, maar dat is ook niet verwonderlijk gezien de omvang en het belang van de eigen defensie- en veiligheids-industrie. Maar Nederland heeft op een aantal thema's meer octrooien dan grote landen als Italië of Spanje. Nederland heeft wereldwijd een sterke positie op beeldverwerking. Deze sterke positie is voor het overgrote deel aan de activiteiten van Philips te danken. Philips is wereldwijd het bedrijf dat de meeste octrooiaanvragen op dit thema doet. Voor beeldverwerking is Nederland over de afgelopen tien jaar de zesde aanvrager (met een aantal van 4,6%). Deze goede positie heeft Nederland ook voor sensoren en ICT. Op het snelgroeiende gebied sensoren neemt Nederland 3% van de octrooiaanvragen voor haar rekening. Dit aandeel blijft iets achter bij wat er gemiddeld gehaald wordt, maar er zit een duidelijke groei in het aantal aanvragen. Philips speelt ook op dit gebied een belangrijke rol, wereldwijd is het de derde aanvrager op dit

gebied. Voor het thema ICT geeft de studie van het Octrooicentrum aan dat er in de onderzochte periode (1995-2005) in totaal 65.459 octrooiaanvragen zijn gedaan op dit gebied. Dit is verreweg het hoogste aantal van de onderzochte thema's. Nederland heeft een aandeel van 3,5% en volgt qua groei het gemiddelde.
Lagere aandelen en ook lagere posities zijn er voor de andere technologieën, al behoort Nederland voor allen tot de top tien wereldwijd met een aandeel van minstens 2,2%.

Impressie van buitenlandse experts

De Technische Wetenschappelijk Attachés uit de diverse landen (China, Duitsland, Frankrijk, Finland, India, Italië, Japan, Korea, Singapore, Verenigde Staten, Verenigd Koninkrijk en Zweden) hebben navraag gedaan naar de reputatie van Nederland op verschillende veiligheidsgerelateerde R&D-gebieden. Daarnaast hebben zij mogelijke samenwerkingskansen in kaart gebracht.[76] Nederland staat internationaal weinig bekend om haar veiligheidsgerelateerde R&D. Landen die sterk zijn op dit terrein zijn primair landen met een grote defensiegerelateerde industrie zoals de Verenigde Staten, Frankrijk, Duitsland en het Verenigd Koninkrijk. Er bestaat in het buitenland geen eenduidig beeld van Nederlandse sterkten op veiligheidsterrein. Duitsland en de Verenigde Staten geven aan dat Nederland bekend staat om haar bescherming van haar kritische infrastructuur onder het motto 'voorkomen is beter dan genezen'. Hierbij wordt vooral gedoeld op de voorzorgsmaatregelen tegen water en de Nederlandse betrokkenheid na orkaan Katrina. Het Zweedse defensie-instituut noemt sensortechnologie, C4I en platformtechnologie als terreinen waarop Nederland een goede reputatie heeft. Nederlandse organisaties die in het buitenland bekend zijn op veiligheidsterrein zijn TNO, Thales, NLR, TU Delft en het NFI. Philips wordt genoemd voor chips en biometrie.
Samenwerking met Nederlandse partijen vindt met name in EU-verband plaats. Frankrijk noemt biometrie, situational awareness en cryptologie als onderwerpen waarop men binnen de EU samenwerkt met Nederland. Het Verenigd Koninkrijk werkt met Nederland samen op het terrein van sensortechnologie.

[75] EZ Informatiecentrum (2007)
[76] TWA (2007)

4 De sterke Nederlandse veiligheidsclusters

4.1 Inleiding

In dit hoofdstuk gaan we in op welke Nederlandse sterke clusters we kunnen onderscheiden op het gebied van Veiligheid. Allereerst bespreken we de technologieën waar Nederland internationaal gezien een sterke positie in heeft. Vervolgens gaan we in op de gehanteerde criteria voor het vaststellen van de Nederlandse veiligheidsclusters. Dit hoofdstuk sluiten we af met de clusters die vanuit een toepassings- en gebruikersperspectief die als internationaal excellent aangemerkt kunnen worden.

4.2 Technologieclusters

Figuur 3 *Technologiegebieden versus toepassingsgebieden*

Toepassingsgebieden	C4I	Operationele besluitvorming	NEC*	Massacom/crowd control	ISTAR**	Defence analysis	Intelligente camera's	Datamining	Simulatie/training/gaming	genereren omgevingsbeeld	Gedrags- en patroonherkenning	Miscellanious defence functions and policy support	CBRNE detectie***	Wapens en munitie	Signatuur beheersing en reductie	Electronic warfare systems & directed energy and technologies	Geïnt Systeemontw.	Equipped personnel	Onbemande systemen	Platforms (bemand)	Identiteitsfraude/virussen/spam	Biometrie/toegangscontrole	Bedrijfsprocessen	Bouwen/gebouwde omgeving
Technologiegebied																			X	X				
Materialen														X	X			X	X	X		X		
Sensoren/sensorsystemen	X		X	X	X		X				X		X	X	X	X		X				X		
Beeldverwerking	X	X		X	X		X				X													
ICT	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**		**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**			**X**	**X**	**X**	
Electrotechniek																X								
Regel- en computertechniek			X	X	X		X		X					X				X	X	X		X		
Milieu veiligheidstechniek																								
Electronica en mechatronica							X		X										X	X				
Werktuigbouwkunde									X					X					X	X				
Medische technologie (Biologisch)													X											
Bouwkunde																						X		
Aandrijving, energiesystemen														X				X	X	X				
Mechanica, hydraulica																			X	X				
Nanotechnologie																								
*Defensie produktietechnologie																								
*Defensie metaalbewerking																								

* Network Enabled Capabilities (NEC): De intentie om sterkere militaire effecten te bereiken door beter gebruik te maken van informatie systemen, met als doel de juiste informatie te verkrijgen, op de juiste plaats, op de juiste tijd, met economisch gebruik van de schaarse middelen.
** ISTAR: Intelligence, Surveillance, Target Acquisition and Reconnaissance

*** CBRNE: Chemical, Biological, Radioactive, Nuclear, Explosive Incidents

In de figuur op de vorige pagina wordt de samenhang weergegeven tussen technologie- en toepassingsgebieden. Deze matrix is breed van opzet en in algemene zin dekkend voor een breed scala aan veiligheidsvraagstukken. De matrix geeft in essentie alle technologievelden (wetenschapsvelden) weer die van belang kunnen zijn in veiligheidsissues. In hoofdstuk 2 is al aangegeven dat één van de karakteristieken van het veiligheidsveld is dat veiligheidstechnologie als zodanig niet bestaat. Bij veiligheid gaat het vooral om de toepassing van bestaande technologie- en/of wetenschapsgebieden. Voor een deel zijn dit meer algemene technologieën die bij een breed scala aan toepassingen een rol spelen. Hieronder worden de belangrijkste besproken, waarin we specifiek ingaan op de mate waarin Nederland zich hierin internationaal onderscheidt.

Beeldverwerking

Voor beeldwerking is al lange tijd aandacht bij universiteiten en kennisinstellingen. Bovendien zijn er op dit gebied grote onderzoeksprogramma's, zoals bij voorbeeld het IOP Beeldverwerking. De internationale positie van Nederland is goed, zo blijkt uit de evaluatie van het IOP in 2004.[77] Met 4,6% van de octrooiaanvragen tussen 1995-2005 neemt Nederland wereldwijd een zesde plaats in.[78] Dat veiligheid een nieuw toepassingsgebied is voor beeldverwerking heeft relatief recent geleid tot plannen voor het oprichten van een community rond 'Veiligheid en Beeldverwerking'. Binnen dit initiatief wordt samengewerkt tussen bijna alle universiteiten en kennisinstellingen samen met een groot aantal bedrijven.

Sensoren

Ook sensoren vormen voor nieuwe veiligheidstoepassingen een belangrijke enabling technologie. Op het gebied van sensoren heeft Nederland van oudsher internationaal een vooraanstaande positie.[79] Ook hier neemt Nederland wereldwijd een zesde plek in qua octrooiaanvragen. De toepassingen liggen vooral op het gebied van life sciences, milieu etc. De kern ligt in Zuidoost Nederland, met partijen als Philips, ASML en TNO. Maar ook Noord-Nederland zet momenteel strategisch in op sensortechnologie, met name via projecten als LOFAR.[80]

[77] B&A Groep (2004)
[78] Octrooicentrum Nederland (2007)
[79] Zie bijvoorbeeld de scriptie van Mathijs Huis in 't Veld (2004) voor een uitgebreide analyse
[80] Samenwerkingsverband Noord-Nederland (2005)

ICT-veiligheid

Op het gebied van ICT-veiligheid (veiligheid-van-ICT) is er bijvoorbeeld het Sentinelsprogramma dat met FES-gelden is gefinancierd. Met het Sentinelsprogramma als basis, is begin dit jaar een nieuw initiatief gevormd met als titel 'Veilig Verbonden'. Binnen dit initiatief wordt samengewerkt tussen bijna alle universiteiten en kennisinstellingen en een groot aantal bedrijven. In hun studie naar Nederlandse R&D in informatie- en netwerkbeveiliging concludeert RAND Europe dat Nederland sterk is op de volgende punten: smartcards; cryptografie; privacy; en beleidsanalyse en veiligheids-consultancy.[81] Nederland is echter zwak op de terreinen ICT-security tools en ondersteunende disciplines (zoals recht, beleid en economie).

Nanotechnologie

Nanotechnologie kan ook toegepast worden voor veiligheidsoplossingen. In de vorm van Point-One, behoort nanotechnologie (vooral nano-elektronica) tot één van de Nederlandse sleutelgebieden. Point-One benoemt veiligheid als één van de toepassingsgebieden. Met bedrijven als Philips, ASML en AMSI is de Nederlandse positie internationaal sterk. De octrooipositie is vooral sterk in de deelgebieden ICT en Biotechnologie binnen de nanotechnologie.[82]

Materialen

Voor het technologiegebied materialen zijn er heel herkenbare veiligheidstoepassingen zichtbaar. Er zijn verschillende onderzoeksprogramma's op dit gebied (geweest), binnen het IOP en bij STW. Er bestaat ook een Technologisch Topinstituut voor materialen: het NIMR. Een compleet overzicht is gegeven in SenterNovem (2007b). SenterNovem concludeert dat in Nederland internationaal toonaangevende bedrijven aanwezig zijn, de wetenschappelijke kwaliteit van hoog niveau is en er veel wordt geïnvesteerd in onderzoek en innovatie. Voor materialen is het innovatieprogramma M2i in ontwikkeling. In dit programma wordt veiligheid als maatschappelijk aandachtsgebied genoemd, al is dit nog beperkt ingevuld.

4.3 Clusters vanuit toepassings- en gebruikersperspectief

Waar is Nederland, internationaal gezien, sterk in op veiligheidsgebied? Welke clusters kunnen vanuit een toepassings- en een gebruikersperspectief onderscheiden worden? Uit gesprekken met experts en vertegenwoordigers van stakeholders (zie bijlage 1), adviezen van TNO en NIID, kwantitatieve analyses naar octrooiaanvragen, wetenschappelijke publicaties en de Nederlandse

[81] RAND Europe (2004)
[82] Octrooicentrum Nederland (2006)

participatie in Europese netwerken, hebben we zeven sterke Nederlandse clusters geïdentificeerd. Dit zijn:

- Detectie, identificatie en authenticatie;
- ICT-veiligheid;
- Command & Control;
- Fysieke bescherming van personen en goederen;
- Situational awareness;
- Onbemande waarneming;
- Simulatie, opleiding en training.

In de volgende paragraaf lichten we deze zeven clusters uitgebreider toe. Hieronder gaan we eerst in op de criteria die we hebben gehanteerd bij het definiëren van deze clusters.

Criteria

De bovenstaande zeven sterke Nederlandse clusters zijn benoemd op basis van:

- De vraag naar innovatieve oplossingen op het gemeenschappelijke gebied van Defensie en Maatschappelijke Veiligheid;
- Het aanbod van innovatieve technologische oplossingen in de vorm van kennis en expertise bij Nederlandse kennisinstellingen en het Nederlandse bedrijfsleven.

Deze clusters zijn alleen dan benoemd als er voor de aanbodzijde aanwijsbaar sprake is van:

- Excellentie: de positie in economisch opzicht, kennispositie en/of wetenschappelijke kwaliteit in internationaal perspectief;[83]
- Samenhang en (internationale) samenwerking: de (potentieel) gemeenschappelijke basis voor de bedrijven en kennisinstellingen, samenwerking tussen bedrijven en kennisinstellingen en aansluiting op relevante internationale netwerken.[84]

We geven geen rangorde aan door onvoldoende beschikbare informatie. Bovendien geldt de excellentie vooral in deelgebieden of specifieke niches zit, waardoor vergelijking tussen de clusters lastig wordt. Deze 'partiële' excellentie moet geplaatst worden in een breder perspectief. Het gaat niet om de onderdelen, maar om het samenstellen van onderdelen en componenten tot een

[83] Er zijn veel sterke buitenlandse bedrijven in Nederland die actief zijn rond Veiligheid. Voor het bepalen van de excellentie zijn alleen díe bedrijven meegenomen waar de voor Veiligheid relevante R&D en innovatie in Nederland plaatsvindt.

[84] Voor het bepalen van de mate van samenhang en (internationale) samenwerking is sterk gekeken naar de bestaande initiatieven en programma's, die in hoofdstuk 3 zijn beschreven.

operationele oplossing. In toenemende mate is er sprake van een internationale supply chain, waarbij onderdelen en componenten ook nog eens uit verschillende landen afkomstig zijn, en de excellentie wordt bepaald door de internationale keten.

Aansluiting op ESRAB-clusters

Afhankelijk van de invalshoek zijn er veel meer clusters te benoemen. In de verschillende defensie-studies is er sprake van meer dan veertig technologiegebieden.[85] Het ESRAB-rapport hanteert elf clusters die qua abstractieniveau goed matchen met de sterke Nederlandse clusters.[86] In Tabel 9 wordt aangegeven hoe de Nederlandse sterke clusters zich verhouden tot de ESRAB-clusters. Daaruit blijkt dat Nederland niet op alle clusters sterk is en per cluster niet over de hele linie.

Tabel 9 *ESRAB-clusters en sterke Nederlandse clusters (bron: Europese Commissie, 2006)*

ESRAB-clusters	Sterke Nederlandse clusters
Risk assessment, modelling and impact reduction	Simulatie, training en opleiding
	Fysieke bescherming van personen en goederen
Doctrine and operation	
Training and exercises	Simulatie, training en opleiding
Detection, identification and authentication	Detectie, identificatie en authenticatie
Positioning and localisation	
Situation awareness and assessment (surveillance)	Situational awareness
	Onbemande waarneming
Information management	ICT-veiligheid
Intervention and neutralisation	
Communication	
Command and control	Command & Control
Incident response	

Aansluiting op voorstellen van NIID, TNO en DIS

De zeven sterke Nederlandse clusters sluiten ook aan op de visie van het NIID over kans voor een innovatieprogramma Veiligheid. Het NIID onderscheidt namelijk de volgende vijf clusters: situational awareness; onbemande systemen; modern en veilig uitgerust personeel; opleiding, training en simulatie; en wetgeving en standaarden.[87] De zeven Nederlandse clusters sluiten verder goed aan op de door TNO onderscheiden vijf belangrijke innovatiekansen voor het thema Veiligheid, te weten: detectie en identificatie van explosieve, chemische en biologische agentia; intelligente sensor-netwerken; bescherming van personen en fysieke objecten; ontwikkelen competenties van

[85] TNO (2006)
[86] Europese Commissie (2006)
[87] NIID(2007)

veiligheidspersoneel en –organisaties; en ICT-Security.[88] Uit Figuur 1 (zie paragraaf 2.3) blijkt daarnaast dat de zeven sterke Nederlandse clusters verder goed aansluiten op de in de DIS benoemde type 1 en type 2 clusters (C4I; Sensorsystemen; Geïntegreerd systeemontwerp en –ontwikkeling; Elektronica en mechatronica; geavanceerde materialen; Simulatie, training en kunstmatige omgevingen).[89]

Geen andere sterke clusters

We benadrukken dat het benoemen van zeven sterke Nederlandse veiligheidsclusters impliciet ook betekent dat Nederland niet sterk is op andere veiligheidsclusters. Dat betekent op zich niet dat er buiten deze zeven clusters geen hoogwaardige R&D en innovatie wordt uitgevoerd of dat er geen bedrijven zijn die internationaal een sterke positie hebben met een innovatief product of dienst. Het betreft dan echter R&D-projecten en/of -bedrijven die hun positie zelfstandig hebben 'veroverd' zonder dat er sprake is van veel samenhang of samenwerking met andere Nederlandse kennisinstellingen of bedrijven. Er is sprake van 'pareltjes'. Een nu nog 'geïsoleerd' pareltje zou natuurlijk in de toekomst kunnen uitgroeien tot een nieuw sterk Nederlands veiligheidscluster.

Relatie veiligheidsvraag en de sterke Nederlandse veiligheidsclusters

De relatie tussen deze toepassingsclusters en de technologie/wetenschapsgebieden wordt weergegeven in Tabel 10. De opzet van deze tabel is een verbijzondering van de matrix aan het begin van dit hoofdstuk waarin de relatie tussen toepassingen en technologie is weergegeven.

[88] TNO (2007)
[89] Ministeries van EZ en Defensie (2007)

Tabel 10 *Relatie veiligheidsvraag en de sterke Nederlandse veiligheidsclusters*

Sterke Nederlandse clusters		Detectie, identificatie en authenticatie	ICT-veiligheid	Command & Control	Fysieke bescherming personen en goederen	Situational awareness	Onbemande waarneming	Simulatie, training en opleiding
Arena Defensie	C41	X		X			X	X
	Sensorsystemen	X				X	X	
	Geavanceerde materialen				X		X	
	Elektronica en mechanica							
	Bescherming en wapensystemen							
	Geïntegreerd systeemonderwerp en -ontwikkeling							
Arena Maatschappelijke Veiligheid	Terrorisme en radicalisering	X						X
	Dreiging-/risicoherkenning en analyse	X						X
	Overlast en kleine criminaliteit	X	X			X		
	Veiligheid van netwerksystemen		X					
	Georganiseerde (internationale) criminaliteit	X						
	Versterking crisisbeheersing			X				X
	Geïntegreerde systemen	X		X		X		
	Uitrusting en materieel				X			

4.4 Zeven sterke Nederlandse veiligheidsclusters

De zeven sterke Nederlandse veiligheidsclusters worden hieronder aan de hand van de eerder genoemde criteria beschreven. Na een algemene omschrijving, waarin het cluster wordt afgebakend, wordt per cluster ingegaan op de relatie met andere clusters, de belangrijkste technologieën, de excellentie en de samenhang en samenwerking binnen het cluster. De beschrijving wordt afgesloten met het benoemen van de belangrijkste partijen. De clusters worden in willekeurige volgorde gepresenteerd, er is geen prioritering aangebracht.

Detectie, identificatie en authenticatie

Het cluster *Detectie, identificatie en authenticatie* vindt zijn toepassing in een nieuwe vorm van waarneming. De hiermee verkregen informatie is vervolgens input voor zowel *command & control* management in meldkamers als voor het ondersteunen van operationeel personeel op locatie. Voor een deel betreft het ook de 'vervanging' van 'blauw op straat' door camera's. Het heeft betrekking op ontwikkelingen zoals (intelligent) cameratoezicht waarbij beeldanalyse wordt toegepast, zowel

decentraal in de camera als centraal in de meldkamer. Ook combinaties met andere detectoren en sensoren, inclusief toepassingen als biometrie (in essentie beeldanalyse, maar dan gericht op het herkennen van personen of persoonskenmerken) vallen onder dit cluster.

- **Andere clusters** die raakvlakken hebben met dit cluster zijn *Command & Control* voor het interpreteren van de (beeld)informatie en het nemen van operationele beslissingen. Met *Situational awareness* zijn er raakvlakken voor het vertalen van informatie naar de operationele werksituatie van veiligheidsmedewerkers op straat (in het veld). Ten slotte zijn er raakvlakken met het cluster *Onbemande waarneming*.
- **Technologisch:** onderwerpen als optiek, sensoriek, ICT-systeemintegratie, beeldverwerking en circuitboards. Daarnaast behoren ook ontwikkelingen in biometrie of through-the-wall radar tot dit cluster.
- De **excellentie** wordt voor een belangrijk deel bepaald door de goede Nederlandse positie in beeldverwerking. Er zijn acht Nederlandse universiteiten (RUG, UT, TU/e, TUD, UL, UM en UvT) en TNO en CWI die zich richten op onderzoek verwant aan dit cluster. In de periode 2005-2007 zijn er 32 publicaties over dit clustergebied verschenen. Uit de analyse van PASR blijkt dat in 2005 op **internationaal** vlak TNO, de TU Delft en het KLPD participeerden in toegewezen projecten. In 2006 namen UC Technologies, TNO en het Ministerie van Financiën deel aan gehonoreerde PASR-projecten. Uit de eerste Security-tender van KP7 blijkt dat TNO, de Universiteit van Amsterdam, het Havenbedrijf Rotterdam en Uniresearch succesvol waren.
- Qua **samenhang en samenwerking** is er een sterke basis in de vorm van de partners in het IOP Beeldverwerking. Vrijwel alle universiteiten en kennisinstellingen en een groot aantal bedrijven nemen hieraan deel.
- **Belangrijke partijen** zijn TNO, Thales, Bosch (voormalig Philips), de Vrije Universiteit, Universiteit van Utrecht, DECIS-lab, NFI, NEDAP, Astron, maar ook kleinere partijen als Sentient, Observision, Sound Intelligence, Vicar Vision, VDG-security en VCS-observation, Bioclear en C-it. Innovatieve starters binnen dit cluster zijn onder andere I-optics, Virus Free Air (spin-off TU Delft), IQ Corporation Announces, C&N, C2V, OpenFortress Digital Signatures, Uniqkey Biometrics en Utellus.

ICT-veiligheid (veiligheid-van-ICT)

Het cluster *ICT-veiligheid* richt zich op de veiligheid van de ICT-infrastructuur en op de beveiliging van de informatie zelf. Het gaat hierbij niet om de inhoud van de informatie. Voor communicatienetwerken zoals internet gaat het om SPAM, virussen, identificatiefraude en phishing. Voor informatiebeveiliging gaat het verder over encryptie of virtual private network (VPN). De veiligheid-van-ICT

is verder een aspect (en dat maakt ook het onderscheid) dat van veel breder belang is voor onze economie en maatschappij. Andere aspecten van dit cluster zijn:

- Dit cluster heeft raakvlakken met vrijwel alle **andere clusters**. Bij bijna alle andere clusters is er sprake van communicatie die kwetsbaar is. Een uitzondering is het cluster *Fysieke bescherming van personen en goedere,* die link is er in mindere mate. Bij de ontwikkeling van een nieuw brandwerend pak voor veiligheidsdiensten dienen in het pak ook communicatiemiddelen geïntegreerd te worden.
- **Technologisch** gaat het om ontwikkelingen in informatie- en ICT-architectuur, meer wiskundige versleutelingstechnieken voor encryptie en programmeertechnieken (die programma's opleveren die minder gevoelig zijn voor virussen etc.).
- Qua **excellentie** is er voor de octrooien op ICT-gebied een redelijk goede positie (zesde plek wereldwijd. Er zijn twintig gerelateerde lopende onderzoeken gevonden. Hierbij zijn zeven universiteiten betrokken (RUN, RUG, TU/e, TUD, UT, VU en de UvT). Ook TNO is actief op dit gebied. Er is één relevante publicatie in 2007 van de TU Eindhoven en de Universiteit van Tilburg gevonden. Uit de analyse van de PASR-projecten blijkt dat op **internationaal** vlak de Radboud Universiteit in 2005 participeerde in een gehonoreerd project gerelateerd aan dit cluster. In de eerste tender van Security binnen KP7, dienden Europol, NORIT Nederland en TNO met succes een voorstel in. Volgens onderzoek van SenterNovem naar R&D in ICT en Veiligheid is de kennispositie van Nederland zeer goed op de deelgebieden: network security, security protocols en secure mobile communication; e-commerce, e-business, PKI (public key infrastructure), digitale handtekening, data-privacy en smartcards.
- De basis voor dit cluster is de **samenwerking** binnen het Sentinelsprogramma en het daarop aansluitende initiatief 'Veilig Verbonden' waarin vrijwel alle universiteiten en kennisinstellingen op dit gebied participeren, samen met een groot aantal kleine en grote bedrijven.
- **Belangrijke partijen** zijn de universiteiten van Twente, Utrecht en Nijmegen, TNO, CWI, Telematica Instituut, Philips, Capgemini en LogicaCMG. Qua kleinere bedrijven kan gedacht worden aan Fox-IT, Kahuna, Securecomm, Intermedia security technology. Innovatieve starters op dit gebied zijn onder meer: Borg Identity, com-Connect Security en SMS4sure.

Command & Control

Dit cluster richt zich op het operationele management bij toezicht en bij incidenten, rampen en crises. Het is een cluster dat ook bij niet-criminele veiligheid van belang is. Incidenten, rampen en crisis kunnen immers ook het gevolg zijn van een ongeluk als het ontsporen van een trein, of een natuurramp zoals overstromingen of wat kleinschaliger een incident als brand door kortsluiting of blikseminslag. Bij *Command & Control* is de centrale aansturing vanuit één locatie waar alle

relevante informatie samenkomt een belangrijk aspect. Intelligent cameratoezicht behoort ook tot dit cluster met als meerwaarde dat het in meldkamers leidt tot informatiereductie.
Naast de technologische kant is de menselijke factor van groot belang. Hoe kan informatie op een passende wijze worden aangeboden? Hoe moeten meldkamers optimaal worden ingericht? Bij crises en rampen spelen werkdruk en stress een rol. Deze aspecten kunnen tot gevolg hebben dat niet alle informatie ook daadwerkelijk aandacht krijgt of goed wordt geïnterpreteerd.

- **Andere clusters:** *Detectie en identificatie* van informatie en *Onbemande waarneming* kunnen input leveren voor command- en controlsystemen. Met *Situational awareness* kan er sprake zijn van informatie-uitwisseling. Met *Simulatie* kan de operationele uitvoering van Command & Control worden geoefend en getraind.
- **Technologisch** gaat het over systeemintegratie: het combineren van informatie en gegevensbestanden, datamining, decision support en communicatie.
- De **excellentie** van dit cluster is lastig te bepalen. Het literatuuronderzoek van EZ wijst op drie onderzoeksgroepen waarin de Universiteit Twente, Wageningen Universiteit en TU Delft, maar ook TNO en de KNAW participeren. Er zijn uit 2005 en 2006 drie publicaties bekend van de TU Delft, TNO en het COT. **Internationaal** gezien blijkt uit de analyse van de PASR-projecten dat in 2005 het KLPD, het NLR, TNO en 42 Solutions BV participeerden in twee met succes ingediende projecten. In 2006 namen Europol en TNO deel aan gehonoreerde projecten op dit gebied. De eerste tender van Security in KP7 wijst uit dat het SCP, Sogeti Nederland, TNO, het Instituut Sociale Studies en de Vrije Universiteit participeren in met succes ingediende projecten.
- **Samenwerking** vindt vooral plaats op projectbasis (zie bovenstaande alinea). Binnen de NIID is er een platform Command, Control and Technologie, waar bedrijven zich hebben verenigd. Daarnaast is het netwerk rond het IOP Mens-Machine Interactie relevant voor dit cluster.
- De basis voor dit cluster ligt bij **partijen** als TNO en Thales. Ook systeemintegrators zoals Imtech en CapGemini zijn hier belangrijke partijen.

Fysieke bescherming van personen en goederen

Dit cluster gaat over het beschermen van personeel en materieel bij incidenten, aanslagen en ander geweld in bedreigende situaties. Het betreft toepassingen als kogel- en steekwerende vesten voor politie en militairen, brandwerende vesten, explosiebestendig straatmeubilair (prullenbakken), catering trolleys voor vliegtuigen, etc.

- Dit cluster is gerelateerd aan de **andere clusters** als het cluster wordt beschouwd als een bredere, geïntegreerde toepassing van de verschillende technologieën, in plaats van alleen

gericht op de fysieke bescherming van personen en goederen. In de bredere benadering heeft het cluster vooral raakvlakken met *Situational awareness*.

- **Technologisch** gaat het vooral om geavanceerde materialen voor toepassingen als kogelvrije vesten en brandwerende pakken.
- De Nederlandse **excellentie** op het terrein van geavanceerde materialen is uitgebreid beschreven door SenterNovem in het nieuwe Innovatieprogramma M2i (materialen).[90] Qua octrooien doet Nederland goed mee op enkele specifieke materiaalgebieden (bijvoorbeeld vezels). Sterke spelers zijn DSM, Akzo Nobel, Teijin Twaron, Ten Cate, Corus en Stork. Drie technische universiteiten en TNO verrichten internationaal erkend onderzoek. Uit literatuuronderzoek blijkt dat in 2005 en 2006 vier gerelateerde publicaties zijn verschenen van de TU Delft en TNO. **Internationaal** gezien blijkt uit de PASR-projecten dat Active Space Technologies in 2006 deel uitmaakte van een consortium dat met succes een project heeft ingediend. TNO was succesvol bij het indienen van een projectvoorstel binnen KP7.
- Voor geavanceerde materialen is de **samenwerking en samenhang** in Nederland goed, maar ook nog in ontwikkeling. Bedrijven en kennisinstellingen zijn al jarenlang verenigd in diverse IOP's en het TTI NIMR. Het nieuwe Innovatieprogramma M2i is breed van karakter en wordt ook breed gedragen. Veiligheid als toepassingsgebied wordt wel benoemd, maar is vooralsnog in beperkte mate aanwezig.
- **Belangrijke partijen** op het gebied van geavanceerde materialen zijn Ten Cate, DSM, Corus, Akzo Nobel, Teijin Twaron, TNO, de drie technische universiteiten, de Erasmus Universiteit Rotterdam, Wageningen Universiteit, NIFV-Nibra, NIMR, Dijkstra, Havenbedrijf Rotterdam, NEDAP en Futura Composites. Kleinere partijen zijn onder andere: Detail Repair, Ecotax, Eefting Inbraakpreventie, HBD Total Security, Heras Mobile Fencing & Security, Infraspecials, North Safety Products, Prefire, Safeworks en Securitech. Innovatieve starters zijn Quintech en TANIQ (spin-off TU Delft).

Situational awareness

Het cluster *Situational awareness* is gericht op het operationeel ondersteunen van veiligheidspersoneel op straat en in het veld. Niet alleen te voet, maar ook in of rond voertuigen. Het betreft mobiele en draadloze toepassingen die informatie verstrekken om beter voorbereid te zijn op incidenten waarmee men geconfronteerd zal worden. Ook de terugkoppeling van informatie naar de meldkamer en/of commandopost voor Command & Control is van belang. De ontwikkeling van PDA's maakt het mogelijk om op snelle en eenvoudige wijze gegevensbestanden te raadplegen. Met PDA's of

[90] SenterNovem (2007b)

beeldtelefoons kan verder visuele informatie over de plaats van delict, waarnaar men op weg is, worden aangeboden (bijvoorbeeld via een beschikbaar camerasystemen). De ontwikkeling voor geografische informatie zoals kaarten en precieze plaats-locatie-informatie zijn ook verbonden aan dit cluster.

- Situational awareness is gerelateerd aan de **andere clusters** *Detectie, identificatie en authenticatie*, *Command & Control* en *Fysieke bescherming van personen en goederen*.
- **Technologisch** betreft dit een breed scala aan ICT-gebaseerde ontwikkeling. Ook ontwikkelingen als First responder, soldier modernization program (SMP) of Verbeterd Operationeel Soldaatsysteem (VOSS) passen binnen dit cluster.
- De **excellente positie** van dit cluster in beeldverwerking uit zich in de octrooien, waarvoor Nederland een heel sterke positie inneemt dan gemiddeld het geval is. Uit literatuuronderzoek van EZ komt naar voren dat er elf lopende onderzoeken zijn gericht op dit gebied. Binnen deze onderzoeken participeren zes universiteiten (RU, TU/e, UT, TUD, UM en VU). Daarnaast nemen TNO en het Holst Centre hieraan deel. Er zijn verder vier gerelateerde publicaties uit 2005 van de technische universiteiten uit Delft en Eindhoven en TNO. **Internationaal** gezien blijkt uit de PASR-projecten dat TNO in 2006 betrokken was bij twee met succes ingediende projecten. TNO was daarnaast ook succesvol in KP7.
- De **samenwerking** in dit cluster vindt plaats via de programma's VOSS en SMP van het ministerie van Defensie.
- **Belangrijke partijen** op dit gebied zijn TNO, TomTom, de technische universiteiten van Delft, Eindhoven en Twente, het Telematica Instituut, de Universiteit van Amsterdam en VTS pn. Een innovatieve starter is Ambient Systems.

Onbemande waarneming

Het cluster *Onbemande waarneming* richt zich op de behoefte om verkenningen uit te kunnen voeren van incidentlocaties zonder het inzetten van menselijke verkenners in vliegtuigen of voertuigen. Het betreft toepassingen als onbemande vliegtuigen en robotachtige voertuigen.

- Het cluster onbemande waarneming is gerelateerd aan de **andere clusters**: *Detectie, identificatie en authenticatie* en *Command & Control***.**
- **Technologisch** gaat het om de toepassing van sensoren, robot motion planning, intelligent gedrag (AI) en multi-agentsystemen (samenwerkende teams). Mechatronica en materiaaltechnologie spelen ook een belangrijke rol. De specifieke Nederlandse expertise richt zich vooral op de complexiteit en innovatie voor het realiseren van kleine vliegtuigjes en robotisering.
- De **excellentie** van dit cluster is sensoren. Het komt naar voren in de octrooien, waar Nederland een redelijke positie inneemt en waar een duidelijke groei waarneembaar is. Philips is ook hier

de belangrijkste Nederlandse aanvrager (derde wereldwijd). Naast Philips zijn ASML, TNO en de Nederlandse vestiging van Mitsubishi de belangrijkste aanvragers. Het literatuuronderzoek van EZ wijst op drie lopende onderzoeken waarin de technische universiteiten Delft en Twente, TNO en de Vrije Universiteit Amsterdam deelnemen. Uit de periode 2005-2007 zijn zes gerelateerde publicaties van de Universiteit van Amsterdam, het Holst Centre, de TU Delft en TNO bekend. Binnen PASR zijn er geen projecten bekend met een Nederlandse deelnemer gerelateerd aan dit cluster. Uit de eerste tender van KP7 blijkt **internationaal** gezien dat het Havenbedrijf Rotterdam en Uniresearch deelnemen aan consortia die met succes projecten hebben ingediend.

- De basis voor het cluster vormt de **samenwerking** binnen Netherlands Industrial MALE UAV Platform (NIMUP)[91] waarin een tiental bedrijven al diverse jaren samenwerkt voor het realiseren van onbemande vliegtuigen. Dit cluster zoekt verbreding naar onbemande voertuigen.
- **Belangrijke partijen** zijn onder meer Thales, TNO, Stork, NLR en het ISLA. Qua materiaaltechnologie zijn ook DSM en TU Delft (vliegtuigbouw) belangrijke partners. Innovatieve starters zijn Delft Dynamics, ISIS BV (spin-off TU Delft) en Airborn.

Simulatie, opleiding en training

Door de steeds geavanceerdere oplossingen en systemen is er een toenemende behoefte aan training en opleiding. Dit cluster gaat over simulatie en serious gaming gericht op het virtueel oefenen voor incidenten, rampen en crises. Voor een goede voorbereiding op terroristische aanslagen is het belangrijk dat er meer operationele ervaring komt zodat adequaat opgetreden kan worden als een dergelijke situatie zich voordoet. Voor deze situaties zijn simulaties interessant, omdat training en opleiding voor situaties die in de praktijk niet tot nauwelijks voorkomen. Dialogic gaat in hun studie in op een aantal cases over veiligheid: virtuele brandweertraining, internetgebaseerde simulatie voor de Politieacademie en e-learning voor het op pijl houden van juridische kennis voor de politie.[92]

- Dit cluster is nauw verbonden met het **cluster** *Command & Control*.
- **Technologisch** gaat het vooral om een breed scala aan softwaretoepassingen uiteenlopend van training en e-learning tot complexe simulatoren en games. Voor simulatietoepassingen gaat het ook om de fysieke, werktuigbouwkundige realisatie van simulatoren zoals vliegtuigcockpits, stuurhuizen van schepen het interieur van auto's.
- Voor de **excellentie** is het beeld niet helemaal duidelijk. In ICIS en GATE lijkt er een goede basis voor de toekomst. Volgens Dialogic en Slot[93] zijn de VS, Canada, Japan en Engeland

[91] zie NIID (2007) en http://www.niid.nl/content.aspx?i=288&p=1
[92] Dialogic (2007)
[93] Slot (2004)

sterker, maar blijft Nederland zeker niet achter, vooral als gaat het om serious gaming. In Nederland zijn er twee onderzoeksgroepen (RUG en TUD) bekend die zich richten op onderwerpen gerelateerd aan dit cluster. Verder wijst het literatuuronderzoek van EZ in de periode 2005-2007 op drie publicaties (TUD, RUG, NLR, UM en COT). **Internationaal** gezien blijkt dat TNO participeerde in 2006 in een PASR-project gerelateerd aan dit cluster. Er zijn geen met succes ingediende projecten binnen KP7 bekend.

- Voor **samenhang en samenwerking** is er een sterke kern: het DECIS-lab. [94] Hierin participeren vrijwel alle relevante universiteiten en kennisinstellingen en een groot aantal grote als kleine bedrijven. Dit DECIS-lab geeft ook invulling aan het ICIS-project. Daarnaast is het GATE-initiatief serious gaming relevant. Binnen het NIID bestaat het Nederlands Industrial Simulator Platform (NISP) waarin vijftien bedrijven geclusterd zijn rond simulatortechnologie. Dit cluster breidt zich uit met bedrijven die erg veel ervaring en expertise hebben met virtual reality.
- Belangrijke **partijen** zijn TNO, Thales, Imtech, TU Delft, Universiteit van Utrecht, Hogeschool Utrecht, Xsens, AGS en Trigion.

[94] DECIS-lab (2006)

5 Aanbevelingen

In dit hoofdstuk presenteren we een aantal aanbevelingen voor het ontwikkelen van een (maatschappelijk) innovatieprogramma Veiligheid. Deze aanbevelingen volgen grotendeels uit de specifieke karakteristieken van Veiligheid en kennis en innovatie (zie hoofdstuk 2) en uit de ervaring van SenterNovem met het opzetten en uitvoeren van innovatieprogramma's. De aanbevelingen zijn:

- Volg een integrale aanpak bij het benoemen en oplossen van knelpunten;
- Versterk de relatie tussen Veiligheid en bestaande initiatieven en programma's;
- Zorg voor coördinatie;
- Sluit aan op KP7 en andere Europese programma's.

Volg een integrale aanpak bij het benoemen en oplossen van knelpunten

Een innovatieagenda is gekoppeld aan een visie en ambitie. De agenda beoogt díe knelpunten op te lossen die het bereiken van deze ambitie in de weg staan. De ervaring met de innovatieprogramma's van het ministerie van Economische Zaken leert dat er veel typen knelpunten kunnen zijn die vragen om een verschillende, aanpak. Naast bekende knelpunten zoals gebrek aan kennis en financieringsmogelijkheden, zien we ook knelpunten als gebrekkige samenwerking, beperkte doorstroom van kennis naar toepassingen, belemmerende wet- en regelgeving, (toekomstig) tekort aan menselijk kapitaal, slechte toegang tot buitenlandse markten en beperkte aansluiting op internationale netwerken. Bij Veiligheid spelen waarschijnlijk het gebrek aan standaardisatie en sociale, organisatorische en ethische factoren een rol. We bevelen aan om bij de innovatieagenda een integrale aanpak te volgen, waarbij álle relevante aspecten worden meegenomen.

Versterk de relatie tussen Veiligheid en bestaande initiatieven en programma's

Verschillende initiatieven en programma's gericht op kennis en innovatie hebben een (potentiële) link met Veiligheid. De overheid investeert al jaren flink in publiekprivate technologieontwikkeling, die uitstekend aansluit op de zeven sterke Nederlandse clusters. Bijvoorbeeld Sentinels, Veilig Verbonden, de innovatieprogramma's Point-One en M2i, de programma's in ontwikkeling Diensteninnovatie en ICT en High Tech Systems, de IOP's Photonic Devices, Self Healing Materials en Mens-Machine Interactie, het GATE-programma en het BSIK-programma ICIS (zie hoofdstuk 3). Sommige van deze programma's en initiatieven hebben Veiligheid als onderwerp in meer of mindere mate benoemd, anderen nog niet. De aanbeveling is om de initiatieven en programma's die raakvlakken hebben met de zeven sterke Nederlandse clusters, te betrekken bij het ontwikkelen van de maatschappelijke innovatieagenda Veiligheid, om zodoende doublures te voorkomen en om nieuwe en onverwachte oplossingen voor Veiligheid in kaart te brengen.

Zorg voor coördinatie

Voor de maatschappelijke veiligheidsbehoefte is een goede vraagarticulatie belangrijk, zodat aanbieders van kennis en oplossingen hierop kunnen inspelen. Een goede aanzet is gegeven via de arena's Defensie en Maatschappelijke Veiligheid en via de Programmadirectie Kennis en Innovatie. Dit betreft echter ook het in voldoende mate betrekken van andere vragers, niet zijnde de overheid zelf, voor veiligheidsvragen die spelen bij het bedrijfsleven en de burger. Veiligheid heeft een breed toepassingsgebied waarop vele aanbieders actief zijn. Er is veel R&D en innovatie op verschillende terreinen die voor Veiligheid relevant kunnen zijn. In deze verkenning is een eerste overzicht hiervan gemaakt. Het is strategisch belangrijk om dit overzicht actueel te houden en aan te vullen waar nodig. Het organiseren van technology assessment, evaluatie, monitoring en 'geleerde lessen' is belangrijk zodat inzichten en ervaringen breed worden gedeeld en wordt voorkomen dat het wiel opnieuw wordt uitgevonden. Op basis van dit rapport kunnen dan relevante verbanden en contacten gelegd worden tussen verschillende initiatieven. Bij het ontwikkelen van een innovatie-programma is een aanspreekpunt noodzakelijk bij het bedrijfsleven en de kennisinstellingen. Dit aanspreekpunt kan een consortium, een platform of een regieorgaan zijn.[95] De vorm is niet het belangrijkste, zolang het maar invulling geeft aan een representatieve inbreng van bedrijven en kennisinstellingen, draagvlak heeft in het veld en inzicht heeft van wat er speelt. Bovendien zou dit aanspreekpunt de rol van aanjager op zich moeten nemen. De ervaring van leert dat er zonder aanjager geen (vraaggestuurde) innovatieprogramma's totstandkomen.

Sluit aan op KP7 en andere Europese programma's

De Europese Commissie zet in KP7 en andere stimuleringsregelingen strategisch in op Veiligheid. Veel terugkomende onderwerpen zijn gerelateerd aan de innovatievraag van Defensie, BZK en Justitie en aan de zeven sterke Nederlandse clusters. Voor KP7 heeft Nederland een goede uitgangs-positie om deel te nemen in het European Security Research Programme (ESRP). In de voorloper (PASR) participeerden meer dan vijftig Nederlandse bedrijven en onderzoeksinstellingen. Andere Europese stimuleringsprogramma's richten zich niet primair op innovatie maar meer op de Europese opschaling en implementatie van veiligheidsoplossingen. Dit heeft ook betrekking op Nederlandse innovatieve ontwikkelingen die in een Europese context ingebracht kunnen worden. We bevelen aan om bij het opstellen van de (maatschappelijke) innovatieagenda te voorzien in een proactieve inbreng in de betreffende programmacommittees (zoals het ESRP) en adviesorganen (zoals het ESRIF), en om het nationale (maatschappelijke) innovatieprogramma rond Veiligheid inhoudelijk aanvullend te laten zijn aan op de Europese programma's.

---

[95] De AWT pleitte in 2003 voor het oprichten van een nationaal regieorgaan Misdaadkennis (AWT, 2003)

Literatuur

Ad hoc Commissie "Brugfunctie TNO en GTI's" (2004), *De kracht van directe verbindingen*, Den Haag, (http://www.senternovem.nl/mmfiles/De%20kracht%20van%20directe%20verbindingen_tcm24-218899.pdf)

AWT (2003), *Kennis van criminaliteit*, Advies 52 van de Adviesraad voor Wetenschaps- en Technologiebeleid (http://www.awt.nl/uploads/files///Adviezen/a52.pdf)

AWT (2007), *Weloverwogen impulsen: Strategisch investeren in zwaartepunten*, Advies 72 van de Adviesraad voor Wetenschaps- en Technologiebeleid (http://www.awt.nl/uploads/files///Adviezen//awt72_weloverwogen-impulsen.pdf)

B&A Groep Beleidsonderzoek & - Advies bv (2004), *Eindevaluatie IOP Beeldverwerking*, Den Haag

Campus Den Haag en Universiteit Leiden (2007), *Internationaal recht, Internationale betrekkingen en veiligheid*, i.s.m. Haagsche Academische Coalitie, TNO Defensie en Veiligheid, TUD en Erasmus Universiteit Rotterdam (http://www.campusdenhaag.nl/documenten/actieplanintrecht.pdf)

CCV (2005), *Samenwerken; eindevaluatie interdepartementale stimuleringsregeling T&S Criminaliteitspreventie*, in opdracht van de ministeries van EZ, BZK en Justitie.

DECIS Lab (2006), *Combined Systems: combining more for crisis management,* programma op het gebied van decision support en simulatie (http://combined.decis.nl/images/deliverables/combined-project-booklet-2006.pdf)

Dialogic (2007), *Serious gaming, sectoroverstijgende technologie- en marktverkenning*, onderzoek door Dialogic in opdracht van EZ, EZ-publicatienummer 07ET09 (http://www.minez.nl/dsc?c=getobject&s=obj&objectid=153488&!dsname=EZInternet&isapidir=/gvisapi/)

ECP.NL (2007), *R&D ICT-security; inventarisatie en richtingen voor vervolg*, onderzoek in het kader van Digibewust, door A. Eisner en M. Viersma (http://www.ecp.nl/download/Rapportage_R&D_ICT-security2.pdf?PHPSESSID=d755c7bf378a)

Europese Commissie (2004), *On the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security research, Towards a programme to advance European security through Research and Technology*, COM(2004)72 final

Europese Commissie (2004b), *Research for a secure Europe, Report of the group of personalities in the field of security research*, EUR 21110

Europese Commissie (2006), *Meeting the challenge: the European Security Research Agenda*, Report from the European Security Advisory Board (ESRAB) (http://ec.europa.eu/enterprise/security/doc/esrab_report_en.pdf)

Europese Commissie (2007), *European Security Research Program (ESRP)*, onderdeel van het 7de Kaderprogramma (http://www-carmin.cea.fr/var/plain/storage/original/media/Emeriau-EC.pdf)

Europese Commissie (2007b), *Towards a general policy on the fight against cyber crime*, Brussels, 22.5.2007, COM(2007) 267 final (http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf)

EZ Informatiecentrum (2007), *Literatuuronderzoek over kennisinstellingen gelieerd aan security,* nr.31708

EZ Informatiecentrum (2007b), *Overzicht van HBO-opleidingen op het gebied van veiligheid*, nr.32957

Federal Ministry of Education and Research (2007), *Research for Civil Security: programme of the German Federal Government* (http://www.bmbf.de/pub/research_for_civil_security_.pdf)

Huis in 't Veld, M. (2004), *Innovation in the sensor technology industry: A policy perspective*, afstudeerscriptie (http://www.studiosus.nl/scripties/00_innovation_sensorindustry.pdf)

ICTRegie (2007), *Veilig Verbonden,* initiatief voor een onderzoeksprogramma gericht op ICT-veiligheid (http://www.ictregie.nl/publicaties/nl_VeiligVerbonden_20May2007.pdf)

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2007), *Onderzoeksprogramma R&D Maatschappelijke Veiligheid*

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en ministerie van Defensie (2005), *Een gemeenschappelijke kennisbasis voor Defensie en Binnenlandse Zaken*, werkgroeprapportage 18 oktober 2005

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en ministerie van Defensie (2006), *Rapportage Intensivering Civiel-Militaire Samenwerking,* Brief van de ministers Remkes en Kamp aan de Tweede Kamer, 24 mei 2006 (http://www.nifv.nl/upload/73193_668_1167753069484-Kamerbrief_Intensivering_civiel-militaire_samenwerking_2006-24mei.pdf)

Ministerie van Economische Zaken (1995), *Kennis in beweging: over kennis en kunde in de Nederlandse economie*, Den Haag

Ministerie van Economische Zaken en ministerie van Defensie (2007), *Defensie Industrie Strategie: eindrapportage* (http://www.niid.nl/file.aspx?i=1349)

Ministerie van Economische Zaken en SenterNovem (2007) *Innovatieprogramma's: volop in bedrijf*, EZ publicatiereeks 07OI36 (http://appz.ez.nl/publicaties/pdfs/07OI36.pdf)

Ministerie van Economische Zaken, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Ministerie van Justitie (2005), *Innoveren is investeren in samenwerken*, eindrapportage van het interdepartementale stimuleringsprogramma Technologie & Samenleving, deelprogramma Criminaliteitspreventie

Ministerie van Economische Zaken, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Ministerie van Justitie (2007), *Herijking ICT-veiligheidsbeleid*, interdepartementaal project

Ministerie van Onderwijs, Cultuur en Wetenschap (2006), *KENNIS VOOR DE SAMENLEVING: Voortgangsrapportage 2006 Implementatie Kabinetstandpunt Brugfunctie TNO/GTI's,* (http://www.minocw.nl/documenten/40350a.pdf)

Nationaal Platform Criminaliteitsbeheersing (2007), *Actieplan Veilig Ondernemen Deel 3: Het bedrijfsleven en de overheid willen samen de criminaliteit tegen het bedrijfsleven terugdringen*, (http://www.justitie.nl/images/Actieplan%20Veilig%20Ondernemen_tcm34-84449.pdf)

Nederland (2007), *Samen werken, samen leven*, Beleidsprogramma Kabinet Balkenende IV 2007-2011 (http://www.samenwerkenaannederland.nl/uploads/ik/cl/ikclUls8PZnZB7wvBquAIQ/Beleidsprogramma.pdf)

Nederland (2007b), *Project Nederland Ondernemend Innovatieland*: *werkprogramma*, Programmadirectie Kennis en Innovatie (http://www.ez.nl/dsc?c=getobject&s=obj&objectid=153186&!dsname=EZInternet&isapidir=/gvisapi/)

NIID (2007), *Van melding naar regie*, notitie aan het projectteam 'verkenning Veiligheid'

Octrooicentrum Nederland (2006), *Nanotechnologie: informatie uit octrooien* (http://www.ocnl.nl/binaries/Rapport_Nanotechnologie_tcm10-8123.pdf)

Octrooicentrum Nederland (2007), *Security: een onderzoek naar de octrooipositie van Nederland* (www.octrooicentrum.nl)

Politie Nederland (2006), *Wenkend perspectief: Strategische visie op politieel informatiemanagement & technologie 2006-2010* (http://www.politie.nl/Overige/Images/33_224352.pdf)

RAND Europe (2004), *Nederlandse R&D in Informatie- en Netwerkbeveiliging: een inventarisatie van onderzoek, trends en uitdagingen in 2004* (http://www.sentinels.nl/library/randsecurity-2004.pdf)

Research voor Beleid (2004), *Sectoranalyse defensiegerelateerde industrie*, onderzoek in opdracht van het ministerie van EZ, nr. B2813 (http://www.minez.nl/dsc?c=getobject&s=obj&objectid=55445&!dsname=EZInternet&isapidir=/gvisapi/)

Samenwerkingsverband Noord-Nederland (2005), *Strategische agenda voor Noord-Nederland 2007-2013* (http://www.snnonline.nl/files/1/%5B1%5Dstrategische_agenda.pdf)

SenterNovem (2004), *Defensie gerelateerde industrie: vertrouwelijk*, Beleidsinteractierapport 2004-19

SenterNovem (2005), *InnovationScan: veiligheid in kennis en toepassing*, Den Haag (http://www.nvso.nl/Innovation%20Scan%20Veiligheid.pdf)

SenterNovem (2006)*, Maritiem: een inventarisatie van de Nederlandse uitgangspositie*

SenterNovem (2007), *Inventarisatie Security R&D in het Nederlandse bedrijfsleven: openbare versie*, Rapportage in het kader van Beleidsinteractie

SenterNovem (2007b), *Innovation Intelligence: High Tech Materialen*

SenterNovem (2007c), *Innovation Intelligence: Chemie*

Slot, M. (2004), *Work in Progress: Nederland in de internationale game industrie*, afstudeerscriptie Media & Journalistiek, Erasmus Universiteit Rotterdam (http://erasmusmedia.net/master/Bestanden/masterthesis%20mijke%20slot.pdf)

TNO (2006), *Innovatiekansen voor de Nederlandse Defensiegerelateerde Industrie, Prioriteiten voor de Nederlandse Defensiegerelateerde Industriestrategie,* TNO 06-IPG-03

TNO (2006b), *Technologieverkenningen maatschappelijke veiligheid 2006*, TNO-DVI 2005 C136, met als preambule de 'Visie op veiligheid en technologie' van BKZ

TNO (2007), *Security als innovatiethema*, notitie aan het projectteam 'verkenning Veiligheid'

TU Delft (2007), *Security in onderzoek en onderwijs bij de TU Delft*, notitie aan het projectteam 'verkenning Veiligheid'

TWA (2007), *Internationale visies op de R&D in Nederland op het gebied van security*, opgesteld door het TWA-netwerk voor het projectteam 'verkenning Veiligheid'

VINNOVA (2005), *Knowledge to safeguard security*, (http://www.vinnova.se/upload/EPiStorePDF/vp-05-03.pdf)

Winsemius, Commissie (2005), *Technologie en misdaad, Kansen en bedreigingen van technologie bij de beheersing van criminaliteit*, advies van de commissie Criminaliteit en Technologie onder leiding van de heer Winsemius, Tweede Kamer 27834, nr. 39 (http://omv.nl/Website/Dutch/nieuws/Aktualiteiten/Advies%20Winsemius.pdf)

bijlage 1 Geïnterviewde personen en organisaties

Tabel 11 *Geïnterviewde personen en organisaties*

Bedrijf/organisatie	Naam
Boon Edam	Dhr. H. van Wijngaarden
Boon Edam	Mevr. B. Smulders
Bosch Security Systems	Dhr. B. Frederiks
Bosch Security Systems	Dhr. H. van der Veen
Capgemini	Dhr. J.S. van Grieken
Capgemini	Dhr. A.W. Huistra
Capgemini	Dhr. J.C.D. van Werkhoven
D-CIS Lab	Dhr. K. Nieuwenhuis
Freeband	Dhr. M. van Buuren
Freeband	Dhr. P. Strating
Honeywell Industrial Solutions	Dhr. E. Richters
VEBON/GE Interlogix	Dhr. H. Wildeman
Politie, ISC	Dhr. M. Nacinovic
KPN Telecom	Dhr. M. Buijs
MultimediaN	Dhr. M. van Worring
MultimediaN	Dhr. A.W.M. Smeulders
Nedap	Dhr. Hogen Esch
NIID	Dhr. R. van Dord
NiiD	Dhr C. van Vliet
NIID	Dhr. M. Kerssen
NIMR	Mevr. L. Hviid
NIMR	Dhr. S. Hoekstra
NLR	Dhr. A.J. Staassen
Politieacademie	Dhr. W. Broer
Rotterdam Port Authority	Dhr. A. Dintjers
Sentinels	Dhr. F. Eisner
Smart Surroundings	Dhr. P. Havinga
Stork	Dhr. M. de Wilde
Telematica Instituut	Dhr. W. Teeuw
Thales Hengelo	Dhr. A. Smits
Thales Hengelo	Dhr. J. Troost
Thales Huizen	Dhr. W. Jongsma
Thales Hengelo	Dhr. L. Roffel
Thales Hengelo	Dhr. A. Hummel
TNO Defensie en Veiligheid	Dhr. J.A. Don
TNO Defensie en Veiligheid	Dhr. P.J. Werkhoven
TNO Kwaliteit van Leven	De heren A.Rensma
TNO Kwaliteit van Leven	Dhr. M. Butter
TU Delft	Dhr. P. Althuis
TU Delft	Dhr. A. Houkes
TU Delft	Dhr. J. de Lange
VCS Observation	Dhr. W. van Dijzen
VEBON/ADI Gardner	Dhr. M. van Kessel
VEBON	Dhr. E. Schoemaker
NVSO/Veilig Verbonden	Dhr. P. Hartel

bijlage 2 Veiligheid R&D bij kennisinstellingen

Als basis voor het onderstaande overzicht het volgende:

- Uitgangspunt is de participatie van universiteiten en kennisinstellingen in nationale en/of Europese programma's en/of projecten. Met name de participatie in Europese projecten geeft aan dat op die onderwerpen er in Nederland excellente expertise aanwezig is. De participatie in Nederlandse projecten geeft aan dat er samengewerkt wordt met andere onderzoeksinstellingen en bedrijven.
- Het overzicht heeft nadrukkelijk alleen betrekking op die projecten en programma's waarbij expliciet sprake is van een veiligheidsinvalshoek. Een aantal programma's zoals PASR, ICIS of Sentinels zijn specifiek gericht op veiligheid (security). Voor de meeste programma's geldt dat deze op programmaniveau weliswaar niet specifiek op veiligheid zijn gericht, maar dat projecten binnen die programma's wel geheel of gedeeltelijk gericht zijn op veiligheid.

Het overzicht geeft daarmee in ieder geval een minimumniveau.

- Het overzicht is nadrukkelijk geen overzicht van faculteiten/vakgroepen die mogelijk een bijdrage aan veiligheid zouden kunnen leveren.
- Het overzicht betreft dus ook geen onderzoeksgroepen die weliswaar inhoudelijk gericht zijn op of betrokken zijn bij veiligheidsonderwerpen maar die verder niet betrokken zijn bij een nationaal of internationaal programma, project of samenwerkingsverband.

Inhoudelijk:

- Onderzoek vindt plaats aan 13 universiteiten (Erasmus Universiteit Rotterdam, Universiteit van Tilburg, Radboud Universiteit, Universiteit Leiden, TU Delft, TU Eindhoven, Universiteit van Utrecht, Rijksuniversiteit Groningen, Universteit Twente, Universiteit van Amsterdam, Vrije Universiteit Amsterdam en Wageningen Universiteit);[96]
- De volgende kennisinstellingen zijn geïdentificeerd: TNO, CWI, NFI, NIBRA, RIKILT, RIVM, NLR, NIMR, ESI en Telematica Instituut. Een bijzondere positie in deze is er voor TNO waar alleen al voor het onderdeel TNO Defensie en Veiligheid 1.060 personen werkzaam zijn. Daarnaast kennen ook andere TNO-onderdelen als ICT en Kennis van Leven veiligheidsgerelateerde eenheden;

[96] Met dank aan TU Delft (2007)

- Uit het overzicht[97] van hbo-opleidingen op Veiligheidsgebied komt naar voren dat er vijf lectoren zijn die zich richten op dit gebied. Het betreft de lectoraten Risicobeheersing (Saxion), Veiligheid en Sociale Cohesie in het publieke domein (Windesheim), Veiligheid, Sociale veiligheid en Fysieke Veiligheid (Hogeschool Zeeland). Daarnaast houdt ook de Politieacademie zich bezig met dit onderwerp.
- Hieronder wordt een overzicht gegeven van kennisinstellingen die actief zijn op het gebied van veiligheid. Naast de naam van de kennisinstelling zijn de Europese en Nederlandse projecten weergegeven waaraan de kennisinstelling deelneemt. Daarnaast is gepoogd inzicht te geven welke onderzoeksgroepen (vakgroepen of capaciteitsgroepen) of welke faculteiten dit betreft en zijn de onderwerpen, indien bekend, weergegeven.

Tabel 12 *Kennisinstellingen actief op het terrein van Veiligheid*

	organisatie	**vakgroep eenheid**	**Europese projecten**	**NL projecten**	**onderwerp**
1	COT	Instituut voor Veiligheids- en Crisismanagement	KP6-TTSRL		terrorisme
2	Criscentrum Leiden		PASR		
3	CWI			MultimediaN	beeldverwerking
4	CWI			IOP-GenCom-BASIS	biometrie
5	CWI	Cryptology and Information Security Research		NWO-VICI, NWO-VENI, BRICKS, Sentinels-PASC	ICT-veiligheid/crypto
6	CWI	Probability Networks and Algorithms (PNA)	KP6-BIOSECURE	NWO-VICI, NWO-VENI, BRICKS, Sentinels-PASC	cryptografie en informatie veiligheid
7	Erasmus Universiteit		PASR-SOBCAH		
8	Erasmus Universiteit		PASR-CASH		
9	Erasmus Universiteit	Medisch Centrum	KP6-RiViGene		forensic
10	KUB			STEVIN Daeso	
11	KUB	Faculteit der Rechtsgeleerdheid	KP6-HUMSEC		terrorisme
12	KUB	Faculty of Law, Center for Law, Public Administra-tion and Informati-zation	KP6-PRIME KP6-Challange KP6-FIDIS		privacy/identiteit
13	NFI	Digital Evidence	KP6-FIDIS		identiteit
14	NIBRA		PASR-INSURA		
15	NLR		PASR/SEC-U-		

[97] Informatiecentrum EZ (2007b)

			AVNET		
			PASR-GEODATA		
			PASR-ENSURE_IT		
			PASR-BDSUAV		
			PASR-HELEVAC		
			PASR-TARAV		
16	Politieacademie		PASR-MGPS		
			Police		
17	Radboud Univ			IOP-GenCom-PAW	privacy
18	Radboud Univ			STEVIN Midas	
19	Radboud Univ	Security of Systems		Sentinels-JASON	ICT-veiligheid
20	Rijksuniversiteit Leiden		PASR-CRIMSON		
21	RIKILT - Institute of Food Safety		PASR-PATHOSENSE		
22	RIVM		PASR-IMPACT		
			PASR-DYNAMOVE		
			PASR-EMC²:IC3		
23	Telematica Instituut			MultimediaN	beeldverwerking
24	Telematica Instituut			Freeband	
25	TNO		PASR-IMPACT		
26	TNO		PASR-ISCAPS		
27	TNO			MultimediaN	beeldverwerking
28	TNO			IOP-GenCom-PAW	privacy
29	TNO		PASR-CM-CATO		
30	TNO		PASR-ROADMAP		
31	TNO		PASR-VITA		
32	TNO		PASR-CODEX		
33	TNO		PASR-SOBCAH		
34	TNO		PASR-CONNECTIVE		
35	TNO		PASR-SENSNET		
36	TNO		PASR-UPSTREAM		
37	TNO		PASR-TARAV		
38	TNO		PASR-HARMONIES		
39	TNO		PASR-PATIN		
40	TNO		PASR-HUMAN		

41	TNO	Defence, Security and Safety	PASR-SAFEST		
42	TNO	FEL	KP6-Airsecure		sensoren
43	TNO	FEL	KP6-GMOSS		omgevingsbeeld
44	TNO	FEL	PASR-SENTRE		
45	TNO	FEL	PASR-DIS		
46	TNO	TNO Bouw & Ondergrond	KP6-L-surf		testcentrum
47	TNO	TNO-Defensieonderzoek	KP6-TTSRL		terrorisme
48	TNO D&V				heel breed
49	TNO ICT			Sentinels- IPID	ICT-veiligheid
50	TNO ICT			Sentinels- PEARL	ICT-veiligheid
51	TNO ICT			Sentinels-S-Mobile	ICT-veiligheid
52	TNO ICT			IOP-GenCom-PAW	privacy
53	TNO ITSEF			Sentinels-PINPAS	ICT-veiligheid
54	TNO Prins Maurits Lab		PASR-SEATOP		
55	TU Delft		PASR-NUMADE		
56	TU Delft		PASR-MUSOR		
57	TU Delft		Sentinel		ICT-veiligheid
58	TU Delft			IOP-GenCom-PAW	privacy
59	TU Delft	Electrical Engineering, Mathematics and Computer Science	KP6-EUROPCOM		omgevingsbeeld
60	TU Delft	Fac. TNW, Quantitative Imaging?	Geen lopende projecten	Cyttron (Bsik), MicroNed (Bsik), SmartCam (STW/Progress), Falcon (Bsik), 4Dwrist (STW), superresolution (TNO)	beeldverwerking
61	TU Delft	LS Mens-Machine Interactie		IOP-MMI-C_at_D	communicatie rampen en crisis
62	TU/e			IOP-GenCom-BASIS	biometrie
63	TU/e	Dept. of Mathematics and Computing Science	KP6-Ecrypt	Sentinels-PINPAS/SEDAN/PEARL	cryptograpie
64	Universiteit.Utrecht		KP6-Challange		privacy
65	Universiteit Utrecht	Instituut voor Marien en Atmosferisch onderzoek Utrecht (IMAU),	KP6-MERSEA		grensbewaking
66	Rijksuniversiteit Groningen	Institute of Mathematics and Computing Science	KP6-PRIME		privacy/identiteit
67	UTwente			MultimediaN-	beeldverwerking

68	UTwente			IOP-GenCom-BASIS	biometrie
69	UTwente			IOP-GenCom-PAW	privacy
70	UTwente			Sentinels- IPID/VRIEND	ICT-veiligheid
71	UTwente	Distributed and Embedded Systems		Sentinels-S-Visper	ICT-veiligheid
72	UTwente	Signals and Systems		Sentinels-ProBiTe	biometrie
73	UvA			STEVIN Daeso	
74	UvA			IOP-beeldverwerking MultiMedian	beeldverwerking
75	UvA	Human-Computer Studies Laboratory		IOP-MMI-TAID	informatiedistributie rampen en crises
76	VU		PASR-ADAPTIVE		
77	VU	Computer Systems Section		Sentinels-DeWorm Sentinels-S-Mobile	ICT-veiligheid
78	Wageningen Universiteit		PASR		

bijlage 3 Internationale onderzoeksprogramma's

In deze bijlage presenteren we in detail een aantal innovatie- en/of onderzoeksprogramma's in andere landen, te weten Finland, Duitsland, Zweden, Oostenrijk, Verenigd Koninkrijk en Frankrijk.[98]

Finland

In Finland is de overheid, via Tekes, in de zomer van 2007 een technologieprogramma gestart en een call geopend op het gebied van 'Safety & security' (hieronder valt bijvoorbeeld ook voedselveiligheid). De Finse overheid ziet een belangrijke internationale markt, waar het land door haar goede kennispositie en beschikbare technologieën een rol kan spelen. De drijfveer lijkt hier, in tegenstelling tot andere landen, veel minder de nationale veiligheid te zijn. De overheid vindt dat er nieuwe netwerken opgebouwd moeten worden tussen Finse systeemontwikkelaars, bedrijven en autoriteiten op het gebied van safety en security. De overheid wil stimuleren dat bedrijven gaan samenwerken met de politie, hulpdiensten en douane. Het programma loopt tot 2012 met een totaal overheidsbudget van 80 miljoen euro, de deelnemende bedrijven en kennisinstellingen dragen aanvullend ook 80 miljoen euro bij.

Voorlopig richt het programma zich op ontwikkeling van systemen die worden gebruikt in crisissituaties en safety en security technologie gerelateerd aan mobiliteit van goederen en mensen. Andere aandachtspunten zijn methoden voor risk assessment en de ontwikkeling van businessmodellen voor de safety en security sector.

Duitsland

Dit jaar presenteerde Duitsland zijn veiligheidsprogramma met de titel "Forschung für die zivile Sicherheit – Programm der Bundesregiering". Het programma loopt in elk geval voor een eerste periode 2007-2010 met een budget van 123 miljoen euro. Het programma valt uiteen in twee programmalijnen. Het eerste programma concentreert zich op scenariogericht veiligheidsonderzoek. Hierin wordt oplossinggericht gewerkt, bijvoorbeeld aan bescherming en redden van mensen, evacuatietechnieken, springstofdetectie, bescherming van infrastructuur (verkeer, energie) en de bescherming van de warenketen. Deze lijn heeft een niet-technologische (onderzoeks)invalshoek. De tweede programmalijn is juist gericht op technologieën. Deze lijn omvat technologieontwikkeling voor een geïntegreerd beschermingssysteem voor hulpdiensten, multi-sensorsystemen voor gevaarlijke stoffen, patroonherkenning en biometrie.

---

[98] Met dank aan het TWA Netwerk

In Duitsland loopt naast dit programma een apart programma (sinds 2003) op het gebied van ICT-veiligheid. Uit de Duitse SWOT-analyse komt naar voren dat de Duitse technologische sterktes zich bevinden op de gebieden: microsysteemtechnologie, ICT, optische technologie, plant en reactor-safety, construction engineering, biotechnologie en sensortechnologie.

Zweden

Het Zweedse advies[99] voor security R&D vindt zijn basis in het Europese veiligheidsbeleid van 2004 en de ervaringen met PASR. Er worden zeven sterke clusters binnen de Zweedse security industrie onderscheiden. Voor een belangrijk deel gaat het om relatieve kleine clusters van enkele tientallen bedrijven. Ter illustratie: het cluster Nucleair Biologisch Chemisch (NBC) telt slechts vier bedrijven, het algemene IT-cluster daarentegen 200. Voor een belangrijk deel gaat het binnen het IT-cluster om kleine bedrijven. Echter, ook bekende bedrijven als SAAB Bofors Dynamics, Bofors Defense, Ericcson, BAe Land Systems Hägglunds en SAAB Aerosystems behoren hiertoe.

Tabel 13 *Zweedse clusters rond security technology (bron: VINNOVA, 2005)*

Cluster	Aantal bedrijven	Aantal werknemers
Complex systems and simulation	19	7.000
IT security	200	2.000
Sensor technology	21	2.000
Mobile solutions	56	2.400
Physical transportation	7	6.600
NBC	4	40
Weapon technology	7	2.000

Zweden heeft inmiddels een programma voor security. Het programma loopt in de periode 2007-2009 en wordt gefinancierd door VINNOVA, de defensie materieel administratie en het Zweedse crisismanagement agentschap. Doel van het programma is om in 2010 het Zweedse onderzoek en de industrie te benutten, zodanig dat ze significant bijdragen aan een verhoogde veiligheid in Zweden en de wereld. Om dit te realiseren moeten onderzoekers en de industrie samenwerken.[100]

[99] VINNOVA (2005)
[100] http://www.vinnova.se/In-English/Activities/Cross-sectoral-issues/Security/

Het onderzoeksprogramma heeft de volgende (sub)doelen:

- Het eenvoudiger maken voor Zweedse onderzoeksgroepen om deel te nemen in Europese onderzoeksprogramma's;
- Faciliteren van deelname in Amerikaanse security onderzoeksprogramma's;
- Innovatiecapaciteit voor de industrie creëren;
- Ontwikkelen van technologie en diensten die uiterlijk in 2010 gedemonstreerd kunnen worden.

Oostenrijk

In Oostenrijk heeft men een nationaal onderzoeksprogramma op het gebied van veiligheid. Het doel is de nationale veiligheid van Oostenrijk en zijn bevolking te verhogen. Het programma is gericht op een samenspel van technologisch, sociaal en geesteswetenschappelijk onderzoek. Er is een budget beschikbaar van 110 miljoen euro in de periode 2005-2013. In de opstartfase was 10 miljoen euro voor 2005/2006 beschikbaar en voor 2007 15 miljoen euro. Er zijn vier programmalijnen:

- Netwerken en verkenningen;
- Gemeenschappelijke R&D-projecten;
- Gemeenschappelijke componentenontwikkeling en demoprojecten;
- Flankerende activiteiten.

Inhoudelijk richt het programma zich in eerste fase alleen op bescherming van de kritische infrastructuur, waarbij naast het voorkomen van materiele schade ook het voorkomen van secundaire schade (sociaal-psychologische schade) centraal staat. Het is niet bekend waarop het programma zich de komende jaren gaat richten.

Verenigd Koninkrijk

De Home Office heeft een "Science and Innovation Strategy" opgesteld voor de periode 2005-2008. De overheid investeert jaarlijks 60 miljoen pond. Voor de komende vijf jaar zijn negen prioriteiten aangemerkt, waaronder: minder misdaad; georganiseerde misdaad stoppen; terrorisme; en meer misdadigers voor het gerecht. In de toekomst verwacht men de volgende technologieën het meest nodig te hebben:

- Identificatie: er is een plan voor een nationale identiteitskaart en er is een Biometric Center of Expertise opgezet;
- Politiewetenschap en -technologie: prioriteiten zijn DNA-analyses om mensen te identificeren en lab-on-a-chip technologie voor forensische analyses op crime scènes en in het lab. Ook imaging technieken worden genoemd en nieuwe manieren om explosieven en wapens te detecteren. Het Verenigd Koninkrijk heeft fors geïnvesteerd om de nationale DNA-database uit te breiden (door DNA af te nemen bij alle verdachten en overtreders). Er

is een speciaal onderzoeksprogramma opgezet om chemische, biologische, radiologisch en nucleaire dreigingen af te weren;
- Tracking technologie (o.a. RFID).

De Home Office werkt vooral met de Forensic Science Service en de Police Information Technology Organisation. De rol van de industrie lijkt niet groot in het programma. De Home Office geeft aan wat er moet gebeuren en verwacht van marktpartijen dat ze hierop anticiperen door nieuwe producten te ontwikkelen. De industrie is vertegenwoordigd in bijvoorbeeld de Police Science and Technology Strategy Group. De politie heeft namelijk een eigen Science Technology Strategy, opgesteld door deze Group.

Frankrijk

In Frankrijk hecht men veel belang aan het onderwerp veiligheid, vanwege de aanslag in de Parijse metro in 1995 en de rellen in de Parijse voorsteden in 2005. De Franse infrastructuur kenmerkt zich door een groot aantal kerncentrales en een sterk ontwikkelde transportinfrastructuur. De technologievelden die daarom in Frankrijk onder de aandacht staan zijn toegangscontrolesystemen en observatiesystemen voor evenementen en vitale infrastructuur. Frankrijk loopt in technologische zin achter op de VS en het Verenigd Koninkrijk in biometrie en de beveiliging van ICT-systemen. De overheid stimuleert betrokken partijen om deze achterstand in te lopen.

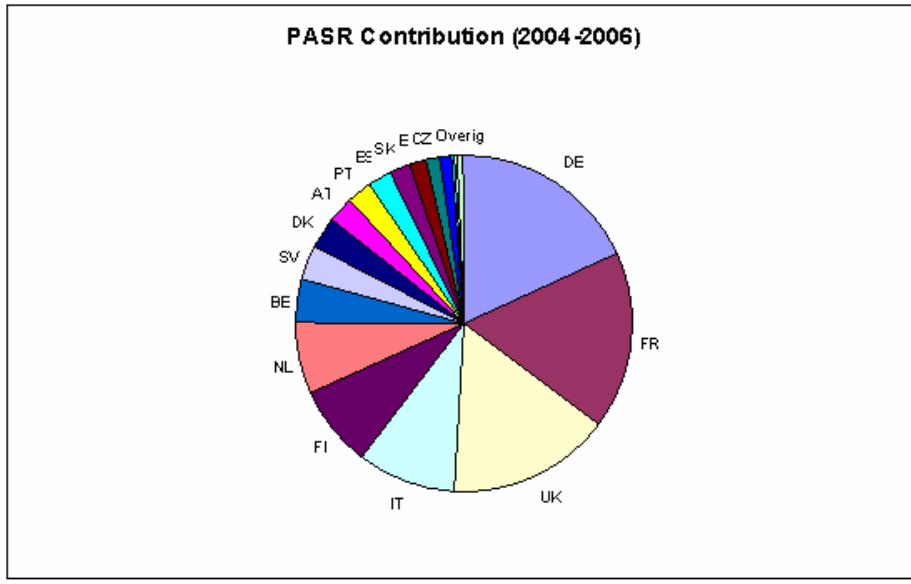
Via het Agence Nationale de la Recherche (ANR) heeft de Franse overheid in 2006 een aanbesteding uitgeschreven om projectmatig onderzoek naar veiligheid te stimuleren. De betreffende projecten zijn veelal publiekprivate samenwerkingsverbanden. Voorbeelden zijn: veiligheid op de Middellandse Zee, defensietechnologie voor burgerveiligheid en EuroCop (efficiëntie van de politie te voet). Frankrijk heeft ook een R&D-programma om detectietechnieken tegen bioterrorisme te ontwikkelen en in de gemeente Elancourt is een proeftuin gestart voor nieuwe veiligheidssystemen.

Verder houden verschillende Franse technologieclusters (Pôles de Compétitivité) zich bezig met veiligheid. Zo is er een Pôle voor de beveiliging van communicatiesystemen, een Pôle voor de verhoging van veiligheid in havens en op zee, een Pôle voor natuurrampenbestrijding, één voor de strijd tegen bioterrorisme en één voor intelligente en proactieve technologie ter beveiliging van openbare ruimten en vitale infrastructuur. Ten slotte de Franse industrie: Frankrijk heeft van oudsher een indrukwekkende defensie-industrie. De drie belangrijkste bedrijven op het gebied van veiligheid zijn Thales, SAGEM en EADS.

bijlage 4 Nederlandse participatie in PASR

In onderstaande figuur geven we de verdeling van beleidsgeld over de verschillende landen. Het blijkt dat Nederland een zesde positie inneemt. In deze bijlage gaan we in op de Nederlandse participatie in PASR.

Figuur 4 *Verdeling PASR-beleidsgeld over verschillende landen (bron: SenterNovem, 2007)*



Tabel 14 *Nederlandse organisaties die hebben deelgenomen aan PASR*

	Organisatie
1	42 Solutions BV
2	Active Space Technologies
3	Association of Traffic Industries in NL
4	Biometric Expertise Group
5	Capgemini
6	Centre for Devel. of Transport and Log.
7	Consultatie Implementatie Technisch beheer BV
8	CPB
9	Crisis Research Center Leiden University
10	Deloitte Accountants
11	DSP-groep
12	Europol

	Organisatie
13	Foundation for Cooperation of Technique and Care
14	Heijmans Infrastructure
15	HSB Cards & Cardsystems BV
16	Joint Aviation authorities
17	Kaba Nederland
18	KEMA Nederland BV
19	Kiwa
20	KLM
21	KLPD
22	LEXISNEXIS Benelux
23	microLAN B.V.
24	Min. BZK
25	Min. Financiën - Tax and Customs Admin.
26	Min. Justitie
27	Netwerk Optimum BV
28	NLR
29	Nuclear Research and consultancy Group
30	Palm Instruments
31	Politie, concern Informatiemanagement
32	Politieacademie
33	Regiopolitie A'dam/Amstelland
34	Respond BV
35	RIVM
36	Stichting Center for Technolog. And Innovation
37	Stichting Katholieke Universiteit
38	Stork Fokker Aerospace
39	Stork WorkSpace
40	Thales
41	TNO
42	TU Delft
43	UC Technologies B.V.
44	Universiteit van Amsterdam
45	Van Riemsdijk R'dam
46	Wageningen University
47	Waternet
48	Westerschelde tunnel

bijlage 5 Nederlandse participatie in KP6 en KP7

Tabel 15 *Nederlandse participatie in KP6 (bron:SenterNovem, 2007)*

Organisatie	Acroniem	Omschrijving
COT-Instituut voor Veiligheids- en Crisismanagement B.V.	TTSRL	Transnational Terrorism, Security and the Rule of Law
Eramus Universitair Medisch Centrum (ERASMUS MC)	RiViGene	Genomic inventory, forensic markers, and assessment of potential therapeutic and vaccine targets for viruses relevant in biological crime and terrorism
Erasmus Universiteit Rotterdam	PRIME	Privacy and Identity Management for Europe
Lactrys Biopharmaceuticals BV	BIODEFENSE	Rapid induction of passive immunity against weapons of bioterrorism using transformed GRAS (generally regarded as safe) microorganisms
Marine Information Service MARIS B.V.	MERSEA	Marine Environment and security for the European Area (MERSEA)
Ministerie van Justitie	FIDIS	The Future of Identity in the Information Society
TNO	AIRSECURE	Risk-based detection and protective filtration system for airports against airborne chemical, biological or radiological hazards
TNO	GMOSS	GLOBAL MONITORING FOR SECURITY AND STABILITY (GMOSS)
TNO	L-SURF	Design Study for a Large Scale Underground Research Facility on Safety and Security
TNO	L-SURF	Design Study for a Large Scale Underground Research Facility on Safety and Security
TNO	TTSRL	Transnational Terrorism, Security and the Rule of Law
Centrum voor Wiskund en Informatica	BIOSECURE	Biometrics for Secure authentication
Stichting Katholieke Universiteit	CHALLENGE	The Changing Landscape of European Liberty and Security
Stichting Katholieke Universiteit Brabant	FIDIS	The Future of Identity in the Information Society
Stichting Katholieke Universiteit Brabant	HUMSEC	Human Security in the Western Balkan region: the impact of transnational terrorist and criminal organisations on the peace-building process of the region
Stichting Katholieke Universiteit Brabant	PRIME	Privacy and Identity Management for Europe
TU Delft	EUROPCOM	Emergency Ultrawideband RadiO for Positioning and COMmunications
TU Delft	SENTINEL	Safety and efficacy for new techniques and imaging using new equipment to support European legislation.
TU Eindhoven	ECRYPT	European Network of excellence in Cryptology
Universiteit Twente	BIOSECURE	Biometrics for Secure authentication
Universiteit Utrecht	CHALLENGE	The Changing Landscape of European Liberty and Security
Universiteit Utrecht	MERSEA	Marine Environment and security for the European Area (MERSEA)
VODAFONE OMNITEL B.V.	POSITIF	Policy-based security tools and framework

Tabel 16 *Nederlandse participatie in KP7 (eerste call, 2007; bron: SenterNovem)*

Organisatie	Project acroniem
Ambulance Zorg Nederland	NMFRDisaster
AVANTES B.V.	OPTIX
European Police Office	EU-SEC II
EUROPOL	Odyssey
Havenbedrijf Rotterdam N.V.	SECTRONIC
Institute of Social Studies	EUSECON
Ministry of Justice	EU-SEC II
NORIT Nederland B.V.	FRESP
SenterNovem	SEREN
Sociaal en Cultureel Planbureau	CPSI
Sogeti Nederland B.V.	CPSI
TNO	CREATIF
TNO	CPSI
TNO	LOTUS
TNO	ADABTS
TNO	DEMASST
TNO	EULER
TNO	FRESP
Uniresearch B.V.	SECTRONIC
Universiteit van Amsterdam	ADABTS
Vrije Universiteit Amsterdam	INEX

bijlage 6 Octrooien Nederlandse bedrijven

Door het Octrooicentrum Nederland is op verzoek van het projectgroep een analyse uitgevoerd van de door Nederlandse bedrijven aangevraagde octrooien op het gebied van veiligheid (security) in de periode 1995-2005.[101] Deze analyse is uitgevoerd op basis van technologiecodes die relevant zijn voor security. Deze relevantie is bepaald aan de hand van de door de projectgroep gedefinieerde technologiegebieden, een vergelijking met de WEAG-taxonomie als ook door het toetsen van een door SenterNovem opgestelde lijst met ruim 200 bedrijven, waarvan bekend is dat deze R&D uitvoeren. Het aantal octrooien door Nederlandse bedrijven en kennisinstellingen aangevraagd is vergeleken met het aantal dat door andere landen is aangevraagd, zodat de internationale positie van Nederland bepaald kon worden. Het octrooionderzoek is uitgevoerd op de volgende technologiegebieden:

- Materialen
- Beeldverwerking
- Elektrotechniek
- Computers
- Sensoren
- ICT

De resultaten per gebied zijn samengevat in Tabel 17. De conclusies zijn:

- Nederland is succesvol in Beeldverwerking. Het aandeel van Nederland is hoog en stijgt sterk. Ook ICT en Sensoren zijn redelijk sterke gebieden met een gemiddeld aandeel en gelijkblijvend of stijgend aandeel.
- Nederland is minder sterk in Elektrotechniek en Computers met een klein aandeel dat daalt of hooguit gelijk blijft.
- In Materialen is het aandeel niet erg hoog, maar het stijgt wel.
- De positie van Nederland is sterk afhankelijk van Philips. Philips is in vijf van de zes sectoren actief en verantwoordelijk voor minimaal tweederde van de aanvragen uit Nederland. De positie van Nederland hangt daarmee heel sterk samen met die van Philips.
- Ontwikkelingen in kleine nieuwe technologieën worden niet zichtbaar. De onderzoeksgebieden zijn vrij breed gedefinieerd. De ontwikkelingen in (kleine) nieuwe technologieën of markten “verdwijnen” in de grote groep.

[101] Octrooicentrum Nederland (2007)

- Het aantal octrooien hoeft niet te betekenen: minder goede octrooien. Het aantal octrooien is geen maatstaf voor commercieel succes of voor de mate waarin een octrooi een doorbraak betekent. Een enkel octrooi kan van groot belang zijn. Dit wordt uit dit onderzoek niet duidelijk.

Tabel 17 *Samenvatting octrooianalyse (overgenomen van Octrooicentrum Nederland, 2007)*

Technologie	Aantal aanvragen wereldwijd	Aandeel Nederland (positie)	Ontwikkeling aandeel Nederland	Grootste Nederlandse aanvragers	
				Grootste aanvragers	Aantal octrooiaanvragen
Materialen	1.700	2,4%	+	DSM	(11)
		(8)		Akzo Nobel	(7)
				Teijn Twaron	(4)
Beeldverwerking	6.200	4,6%	++	Philips	(220)
		(6)		KPN	(12)
				TomTom	(7)
Elektrotechniek	7.400	2,2%	0	Philips	(90)
		(9)		Nedap	(6)
				TNO	(5)
Computers	12.500	2,2%	-	Philips	(167)
		(7)		Nedap	(12)
				TomTom	(10)
Sensoren	18.000	3,0%	+	Philips	(349)
		(6)		ASML	(11)
				TNO	(11)
ICT	65.500	3,5%	0	Philips	(1.765)
		(6)		KPN	(122)
				Irdeto Access	(28)

bijlage 7 R&D door Nederlandse bedrijven

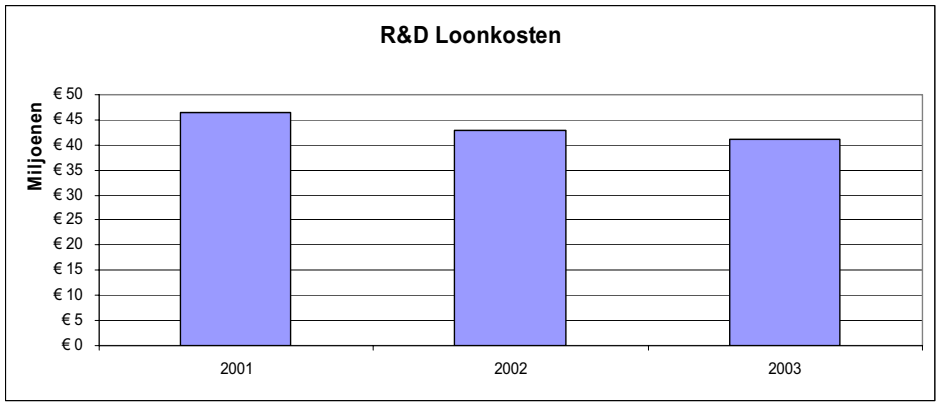
Om een beeld te schetsen van de R&D-inspanningen op het gebied van veiligheid bieden twee studies van SenterNovem naar respectievelijk de defensiegerelateerde industrie[102] en security industrie[103] inzicht. In deze bijlage gaan we in op de in deze beide studies beschreven inventarisatie van relevante projecten die zijn gehonoreerd volgens de Wet Bevordering Speur- en Ontwikkelingswerk (WBSO).[104]

De studie naar de R&D-inspanningen van de defensiegerelateerde industrie gaat over de periode 2001-2003 en de studie naar de veiligheidsindustrie behandelt de periode 2003-2005. Al zijn de beide perioden niet gelijk en is het moeilijk om over een periode van drie jaar uitspraken over trends te doen, toch komt in beide onderzochte perioden voor de twee industrieën een redelijk stabiel beeld van de R&D-inspanningen naar voren. Belangrijk is dat in beide studies alleen projecten zijn meegenomen waarbij in de projectomschrijving expliciet of duidelijk herkenbaar gesproken wordt van een defensiegerelateerde, of een veiligheidsgerelateerde toepassing. In het onderzoek naar de defensiegerelateerde industrie is daarnaast gewerkt met een shortlist. Beide studies schetsen dus de ondergrens van de R&D-spanningen door bedrijven van deze twee industrieën in strikte zin en geven hiermee een indicatie inspanningen door bedrijven op het gebied van de defensiegerelateerde en veiligheidsindustrie.

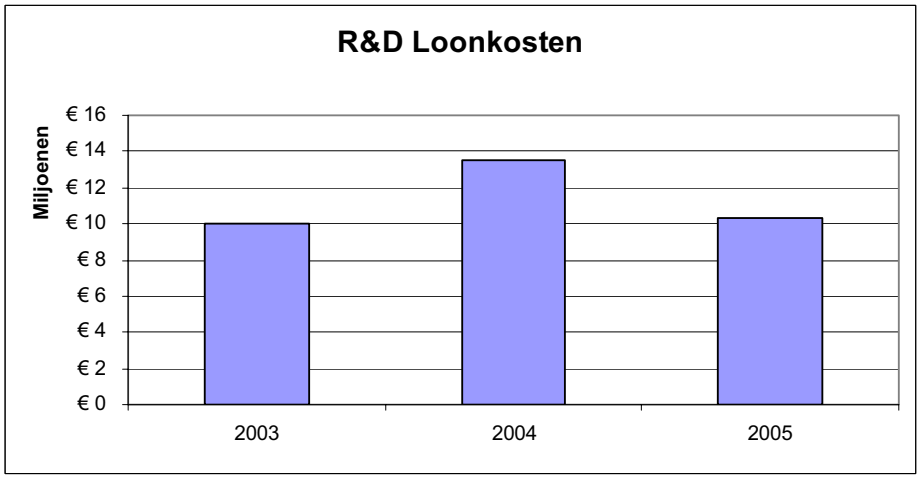
In Figuur 5 en Figuur 6 zijn de R&D-loonkosten per jaar opgenomen voor respectievelijk de defensiegerelateerde en de veiligheidsindustrie op basis van de WBSO. Figuur 5 laat zien dat het in de defensiegerelateerde industrie gaat om een ca. 40 miljoen euro aan R&D-loonkosten per jaar en dat dit bedrag licht lijkt af te nemen. Figuur 6 laat zien dat in de veiligheidsindustrie gaat om een bedrag van gemiddeld tien miljoen euro aan R&D-loonkosten per jaar, met een uitschieter van veertien miljoen euro in 2004. In verhouding tot de totale R&D-loonkosten in de WBSO van 2,1 miljard euro per jaar (2005) bedragen de totale R&D-loonkosten van beide industrieën ongeveer 2,5% van de totale R&D-loonkosten.

[102] SenterNovem (2004)
[103] SenterNovem (2007)
[104] De WBSO is een fiscale stimuleringsregeling voor speur-en ontwikkelingswerk.

Figuur 5 *R&D-loonkosten van defensiegerelateerde industrie (bron: SenterNovem, 2004)*



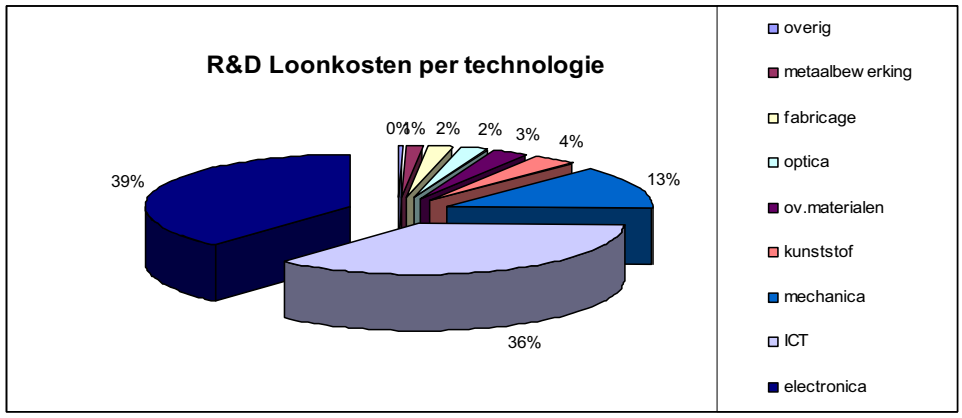
Figuur 6 *R&D-loonkosten van Nederlandse veiligheidsindustrie (bron: SenterNovem, 2007)*



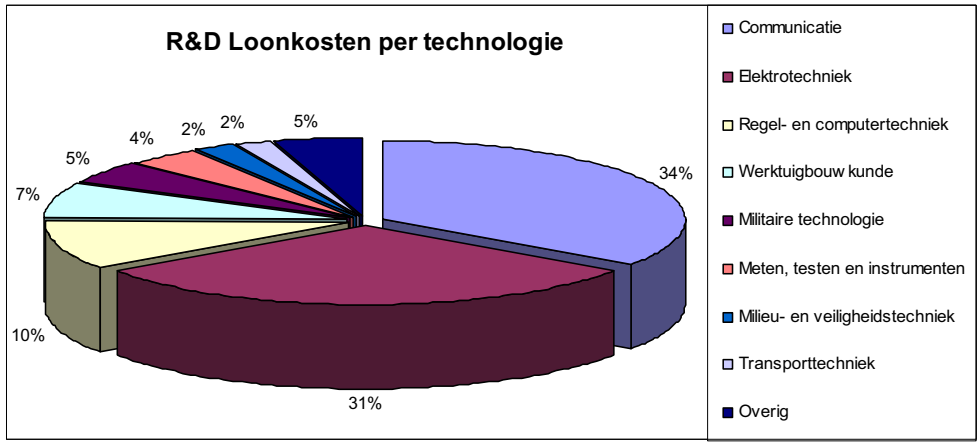
Technologieën

In de beide onderzoeken zijn ook de technologiegebieden waarop de geselecteerde projecten betrekking hebben in kaart gebracht (zie onderstaande figuren).

Figuur 7 *Verdeling van R&D-loonkosten defensiegerelateerde industrie naar technologie (bron: SenterNovem, 2004)*



Figuur 8 *Verdeling van R&D-loonkosten veiligheidsindustrie naar technologie (bron: SenterNovem, 2007)*



Uit Figuur 7 blijkt dat elektronica en ICT veruit de meest dominante technologieën zijn waarop R&D binnen de defensiegerelateerde industrie wordt verricht. In 20% van de R&D-inspanningen wordt onderzoek verricht naar mechanica (werktuigbouwkunde). Er is nog een behoorlijk aantal projecten dat zich (vaak naast andere technologieën) richt op kunststoftechnologie (voornamelijk composieten) en optica, maar deze projecten zijn qua omvang marginaal. Figuur 8 laat zien dat binnen de veiligheidsindustrie in vergelijking met de defensiegerelateerde industrie, onderzoek zich richt op andere technologieën. Communicatie en elektrotechniek nemen bijna tweederde van de

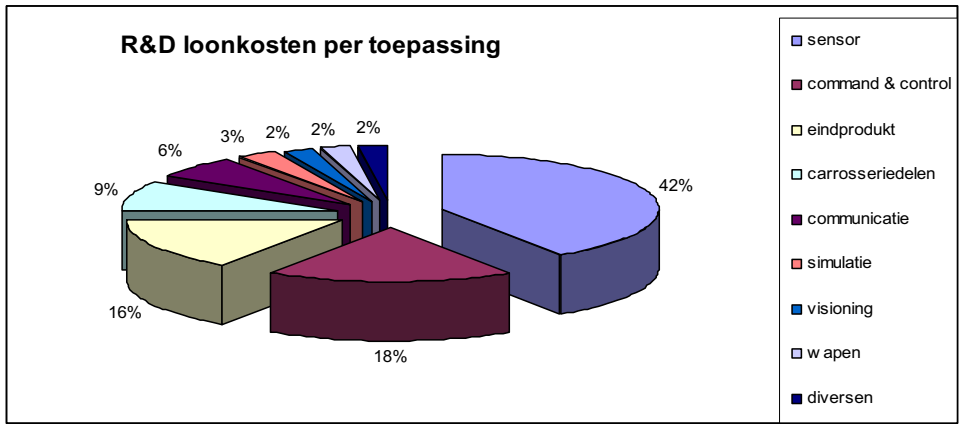
loonkosten voor hun rekening. Hoewel de R&D-activiteiten die als defensiegerelateerd werden geclassificeerd in dit onderzoek buiten beschouwing zijn gelaten, blijkt 5% van de loonkosten naar militaire technologie te worden geclassificeerd.[105]

Toepassing

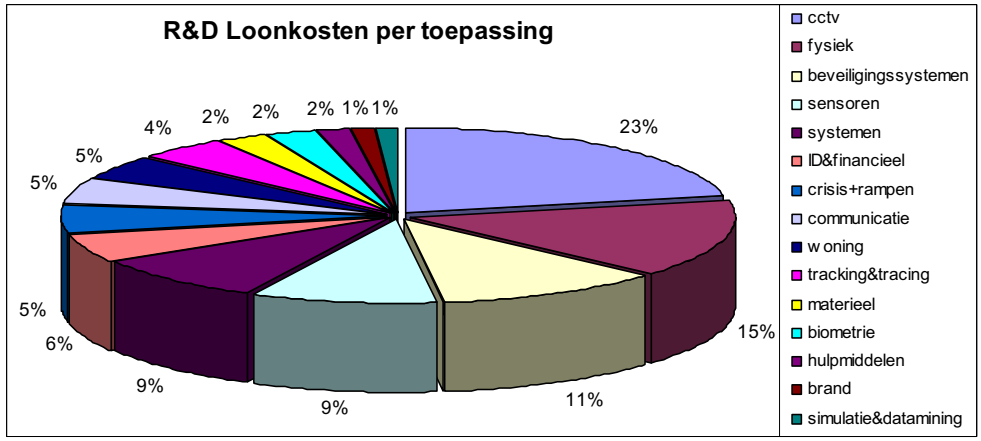
Naast een uitsplitsing in technologieën zijn de projectkosten ook ingedeeld in toepassingsgebieden. In de onderstaande figuren is de verdeling weergegeven van de R&D-loonkosten naar de verschillende toepassingen voor de defensiegerelateerde en respectievelijk de veiligheidsindustrie. In Figuur 9 is te zien dat 42% van de R&D-inspanningen van de defensiegerelateerde industrie is gericht op sensoren. Hieronder valt ook R&D gericht op radar en sonar. Onderzoek naar producten waarin infraroodsensoren worden gebruikt, wordt gerekend tot de categorie visioning. Het gaat daarbij om beeldvormende instrumenten zoals (navigatie-) camera's, nachtkijkers en dergelijke. Command & controlsystemen nemen een prominente tweede plaats in. Daarnaast richt 16% van de inspanningen zich op een direct eindproduct. In deze gevallen is er geen onderscheid te maken tussen het product, waarop het R&D-project betrekking heeft, en het product waarin dit uiteindelijk zijn toepassing zal vinden. Het merendeel van de projecten die hieronder vallen zijn onderzoeken naar wapensystemen. Figuur 10 toont de R&D-loonkosten per toepassing voor de veiligheids-industrie. Hieruit blijkt dat bijna een kwart van de R&D-loonkosten wordt besteed aan onderzoek naar camerasystemen, aangeduid met CCTV (Closed Circuit Television). De tweede toepassing ligt in de sfeer van fysieke (object-)beveiliging, zoals toegangsdeuren. De derde toepassing is beveiligingssystemen. Met deze categorie wordt niet-fysieke (object-) beveiliging bedoeld. Het gaat dan om beveiligingssystemen van ondernemingen en instellingen, zoals professionele alarm- en bewakingssystemen. De categorie woning is hieraan gerelateerd, al is dan gericht op particulieren. De vierde categorie sensoren betreft niet alleen de R&D voor individuele sensoren, maar ook het (detectie-)system waarvan ze onderdeel uitmaken. De detectie van personen maakt in verschillende vormen deel uit van diverse andere categorieën, zoals biometrie, CCTV, beveiligingssystemen en tracking & tracing. De meer traditionele materialen voor in hoofdzaak bestrijding en anderzijds relatief nieuwe, vaak op preventie gerichte, technologieën als biometrie, tracking & tracing en simulatie/datamining kennen een bescheiden omvang aan R&D-loonkosten.

[105] Een verklaring hiervoor is dat bepaalde bedrijven al hun projecten op een bepaald onderwerp standaard van dezelfde technologiecode voorzien.

Figuur 9 *Verdeling van R&D-loonkosten van defensiegerelateerde industrie naar toepassing (bron: SenterNovem, 2004)*



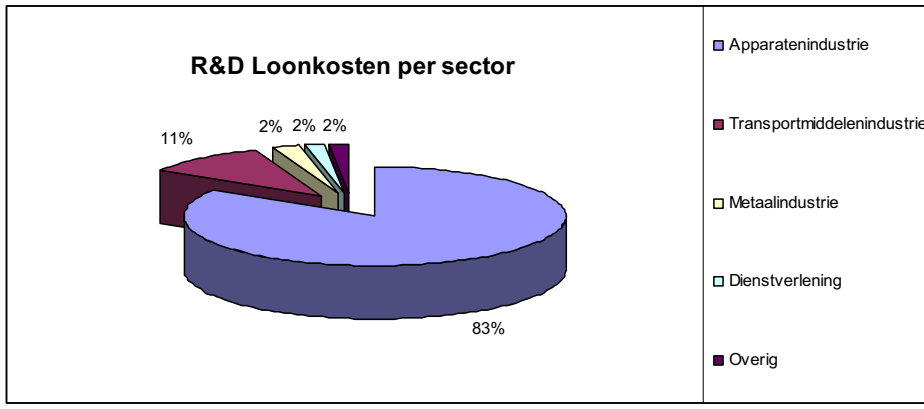
Figuur 10 *Verdeling van R&D-loonkosten van veiligheidsindustrie naar toepassing (bron: SenterNovem, 2007)*



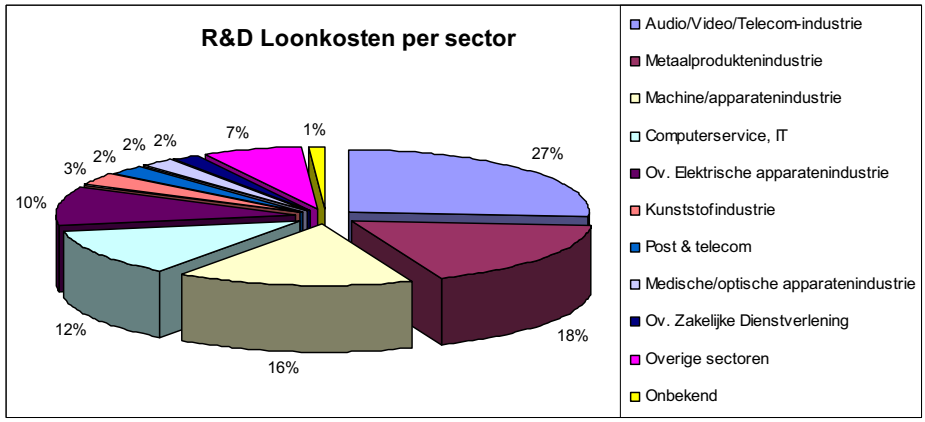
Sectoren

Tot slot bespreken we kort in welke sectoren de bedrijven van de geselecteerde projecten zich bevinden. In de onderstaande figuren is de indeling naar sectoren voor de defensiegerelateerde en respectievelijk de veiligheidsindustrie weergegeven.

Figuur 11 *Verdeling R&D-loonkosten van defensiegerelateerde industrie naar sector (bron: SenterNovem, 2004)*



Figuur 12 *Verdeling R&D-loonkosten van veiligheidsindustrie naar sector (bron: SenterNovem, 2007)*



Het blijkt dat het overgrote deel van de defensiegerelateerde industrie behoort tot de apparatenindustrie. Een belangrijke opmerking hierbij is dat de classificatie van Thales sterk bepalend is voor dit resultaat, gezien de grote omvang van hun defensiegerelateerde R&D-loonkosten. De veiligheidsindustrie laat een ander beeld zien: ruim een kwart van de R&D-loonkosten is afkomstig van bedrijven die tot de Audio/Video/Telecom-industrie worden gerekend. Naast de Machine- en Apparatenindustrie zijn ook de Metaalproductenindustrie en de IT grote sectoren.

bijlage 8 Overzicht Nederlandse bedrijven

In deze bijlage wordt vanuit diverse bronnen een overzicht van Nederlandse bedrijven gegeven die actief zijn op het terrein van Veiligheid.

Tabel 18 *Ledenlijst NIID (bron: www.niid.nl)*

Organisatie		
3-Angle	Geomatics Business Park	RENA electronica BV
3M Nederland BV	Getronics-PinkRoccade	Respond BV
3teQ Industrie	Halin bv	Road Air
Aalberts Industries Defence Technologies	Hawo B.V.	Robert Bosch B.V.
Aarding Special Products BV	Heli-One Components	Robusta B.V.
Acal Nederland BV	Hewlett Packard Nederland BV	Rohde & Schwarz Nederland BV
ACD Salvage Techniek BV	HIAB B.V.	SAFT Batterijen BV
Addit B.V.	High Voltage Potting & Coating B.V.	SAP Nederland BV
Adimec Advanced Image Systems BV	Hitachi Data Systems Nederland BV	Satellite Services BV
AD-S&Co B.V.	HITT Holland Institute of Traffic Technology BV	Scania Production Zwolle B.V.
ADSE Consultancy & Engineering Services BV	Holland Composites Industrials BV	SCC Services BV
Aeronamic B.V.	Hollandia BV	Schelde Marinebouw BV
Airborne Composites	IBM Nederland BV	Scholten Awater B.V.
Alcatel-Lucent	ICT Solutions BV	Siemens Nederland NV
AMCA Hydraulic Fluid Power BV	IFS Netherlands BV	Siemens PLM Software
AOES Group BV	iLionX Group B.V.	SKF Asset Management Services
Askové Kunststof Industrie BV	Imtech Marine & Offshore BV	Stepco Group
Assensys B.V.	Incontrol Enterprise Dynamics	Stork Aerospace .
Atos Origin Nederland BV	INQA Quality Consultants BV	Stork Aerospace.
ATS Kleizen B.V.	Inter (VCD) BV	Stork Fokker AESP - Special Products - Hoogeveen
Autron B.V.	JDR Smart Solutions	Stork Fokker ELMO
Axxiflex Turbine Tools B.V.	JTAG Technologies BV	Stork Fokker Services
Azteco electronics b.v.	Kin Machinebouw Rijen B.V.	Stork NV
Bata Nederland B.V.	Klein Poelhuis Special Projects B.V.	Stork PWV
Bayards Aluminium Constructies B.V.	KPN Telecom BV	Stork SP Aerospace BV
Be Value B.V.	Laktechniek Hengelo B.V.	Stork Special Products BV
Bolidt Kunststoftoepassing b.v.	Lamers High Tech Systems	Sun Electric Systems BV
Bosch Rexroth BV	Landustrie Sneek BV	Sun Microsystems Nederland BV
Brookx Company B.V.	Lankhorst/Pure Composites BV	SurCom International BV
BT Nederland N.V.	Leuveco Technische Handelsonderneming BV	Technamics Manufacturing & Engineering BV
CA Software BV	LogicaCMG Nederland BV	Tecnovia PSM BV
Canon Nederland N.V.	M&I/PARTNERS bv	Tedopres International B.V.
Capgemini Nederland BV	Machinefabriek Bouman B.V.	Teijin Twaron BV

Organisatie		
Carnegie Consult B.V.	Machinefabriek Douna BV	Tele2-Versatel
Castor Networks B.V.	Machinefabriek Elburg BV	Ten Cate Advanced Composites BV
Centric Software Engineering B.V.	Machinefabriek Etten-Leur BV	Ten Cate Advanced Textiles bv
CEVA Logistics Benelux B.V.	Madera Ribs B.V.	Terberg Techniek BV
Cisco Systems International BV	MAFO Holtkamp BV	Terma BV
ComtechDDS BV	Maintenance by EML	Thales Cryogenics BV
CSC Computer Sciences BV	Meilink Industriële Verpakkingen BV	Thales Land & Joint Systems
Cyclomedia Technology B.V.	Merwede Shipyard BV	Thales Nederland BV
Daedalus Aviation Group	Moog FCS Simulator Systems BV	TNO Defensie en Veiligheid
DAF TRUCKS N.V.	MSC Software Benelux BV	TriOpSys BV
DaimlerChrysler Nederland BV	Munters BV	Triview Technical Communication B.V.
De Boer Tenten B.V.	Nationaal Lucht- en Ruimtevaartlaboratorium	TSS International B.V.
Dell B.V.	NCIM-Groep	Turnaround Communicatie
Dutch Defense Vehicle Systems B.V.	Nederlands Centrum voor Laser Research BV	Tyco Electronics Nederland BV
Dutch Space	Nedinsco BV	Tyco Fire & Integrated Solutions
DutchAero BV	Nedtech Engineering BV	Van Halteren Metaal BV
Egmond Plastic BV	Network Appliance B.V.	Van Riemsdijk Rotterdam
Eldim BV	Nevesbu B.V.	Variass Systems B.V
Elinex Power Solutions BV	Neways Defence Electronics	VDL Industrial Modules
EMC Computer Systems BV	Opleidingscentrum Haaglanden BV	Verebus Engineering BV
Enterprise Control Systems B.V.	Ordina Public BV	Verolme Elektra BV
Eonic	OSPL Nederland B.V.	Vicrea Solutions B.V.
ESRI Nederland BV	Perot Systems Nederland BV	Vigilance B.V.
Faes Group BV	PHI DATA B.V.	Vision Waves Aviation & Defence Consulting B.V.
Fijnmechanische Industrie Noord Nederland BV	PHOTONIS Netherlands B.V.	VolkerWessels Netwerk Bouw B.V.
Fox-IT BV	ProSystems International BV	Wilkens c.s.
Fujitsu Services B.V.	Recticel Technical Foams	Xantic BV (a Stratos company)
Futura Composites BV	Reef Precisie B.V.	Yachtgroup Nederland BV
Gemco Mobile Systems BV	Re-lion	Zenitel Netherlands BV

Tabel 19 *Innovatieve MKB'ers op het gebied van veiligheid (bron: Syntens)*

Organisatie	
Adimec	Koninklijke Nederlands Reddings Maatschappy
Arplacon	Lasertec
ASTRON	Nedap
Autec Europe B.V	Nedinsco
Beveiligingsorganisatie Mennega	Neo
Bocasys	Nofiq
Bosch Security Systems	North Safety Products
Bosch Security Systems B.V.	Pape Rietdekkers B.V.
BySpy Products BV	Parabots
CIT group	Parkingware

Organisatie	
CLB Benelux	Parkmanagementvereniging Noordenveld
Dacolian	Prefire
Delft Dynamics	Safeworks
DelftTech	Securecomm
Detail Repair	Securitech
DySI	Sentient
Ecotax	Sound Intelligence
Eefting Inbraakpreventie	Tildesign
Fair Beveiliging	TNO ICT
Fox-it	Trigion beveiliging
HBD Total Security	Van den Broek Beveiligingstechniek en Telecommunicatie
Heras Mobile Fencing & Security	VDS Security Systems
Heras Products B.V.	Ventil Test Equipment
ICT-veiligheid	Vest -it
Infraspecials	Vicar Vision
Intermedio security technology	Joop Wenstedt
I-Products	Zegers
Ivo van Ham	

Tabel 20 *Technostarters op het gebied van veiligheid (bron: TechnoPartner)*

Organisatie
IQ Corporation Announces
Airborn
Delft Dynamics
Quintech
C&N
Borg Identity
Com-Connect Security
SMS4sure
Ambient Systems
C2V
OpenFortress Digital Signatures
Uniqkey Biometrics
Utellus

bijlage 9 Afkortingen, terminologie en begrippen

Afkorting	Omschrijving
Arena	Vraagarticulatie innovatiebehoefte in de uitwerking van de arena Maatschappelijke Veiligheid in het kader van de vraagsturing TNO/GTI's en het onderzoeksprogramma Technologie en Veiligheid (RDMV) regievoering ministerie van BZK
BSIK	Besluit Subsidies Investeringen Kennisinfrastructuur
C4I	Command, Control, Communication, Computers & Intelligence
CCTV	Closed Circuit Television
CCV	Centrum voor Criminaliteitspreventie en Veiligheid. Het CCV is het centrale centrum dat kennis en samenhangende instrumenten ontwikkelt en implementeert om de sociale veiligheid te vergroten.
CODEMA	Commissie Ontwikkeling Defensie Materiaal
Commissie Wijffels	Commissie onder leiding van Herman Wijffels die is ingesteld op verzoek van OC&W minister Maria van der Hoeven voor de toekomstige rol van (Grote) Technologische Instituten. De commissie Wijffels bracht in 2004 het advies "Brugfunctie TNO en GTI's" uit.
COT	Instituut voor Veiligheids- en Crisismanagement
COTS	Commercial of the Shelf
CWI	Centrum voor Wiskunde en Informatica
DECIS	Delft Cooperation on Intelligent Systems
DIS	Defensie Industrie Strategie
ECP.NL	Electronic Commerce Platform Nederland, Platform voor eNederland.
EDA	European Defense Agency
ENISA	European Network and Information Security Agency (enisa.europa.eu)
ESI	Embedded Systems Institute
ESRAB	European Security Research Advisory Board.
ESRP	European Security Research Programma, onderdeel van KP7
EUR	Erasmus Universiteit Rotterdam
FES	Fonds Economische Structuurversterkingen
GTI's	Grote Technologische Instituten
ICTRegie	Publiekprivate samenwerking voor coördinatie van ICT-onderzoek
IIP	ICT-Innovatieplatform
IOP	Innovatiegerichte Onderzoeksprogramma's
ISIS	Interactive Collaborative Information Systems
JLS	Justice, Liberty en Security, Europees DG voor Justitie en Binnenlandse Zaken (JBZ), in het Frans Justice et Affairs Interieur (JAI)
JSF	Joint Strike Fighter
KNAW	Koninklijke Nederlandse Akademie van Wetenschappen
KP	Kaderprogramma; groot onderzoeksprogramma van de Europese Commissie
KLPD	Korps Landelijke Politiediensten
LBVM	Landelijk Bureau Voorkoming Misdrijven
M&ICT	Maatschappelijke Sectoren en ICT. Interdepartementaal programma met als doel de opschaling van succesvolle ICT-initiatieven.
MOOTW	Modus Operandi Other Than War
NBC	Nucleair, Biologisch en Chemische. Typering van soorten wapens. Veelal ook breder aangeduid met NBRC of NBRCE; R = radioactief, E = explosive incidents

NCC	Nationaal Coördinatie Centrum. Het NCC verzorgt de informatievoorziening tussen de verschillende bestuurslagen en, als er buitenlandse aspecten meespelen, voor de contacten met de ons omringende landen in geval van orde- en veiligheidsmaatregelen op centraal niveau.
NCTb	Nationaal Coördinator Terrorismebestrijding. De NCTb is aangesteld om de samenwerking tussen instanties die betrokken zijn bij terrorismebestrijding te verbeteren.
NFI	Nederlands Forensisch Instituut
NIBRA	Nationaal Instituut Fysieke Veiligheid Nibra
NIID	Stichting Nederlandse Industriële Inschakeling Defensieopdrachten
NIMR	Netherlands Institute for Metals Research
NIMUP	Netherlands Industrial “Medium Altitude Long Endurance Unmanned Aerial Vehicle” (MALE UAV) Platform.
NISP	Nederlands Industrial Simulator Platform
NLR	Nationaal Lucht- en Ruimtevaartlabaratorium
NPC	Nationaal Platform Criminaliteitsbeheersing.
NVSO	Nationaal samenwerkingsVerband Security Onderzoek
PASR	Prepatory Action Security Research. Europees stimuleringsprogramma voor de periode 2004-2005. Heeft in 2007 een vervolg gekregen in de vorm van een security thema European Security Research Programma (ESRP)als onderdeel van KP.
PIP	Politie Innovatieprijs
RIKILT	Instituut voor Voedselveiligheid is een onafhankelijk onderzoeksinstituut op het gebied van veilig en gezond voedsel.
RIVM	Rijksinstituut voor Volksgezond en Milieu
RUG	Rijksuniversiteit Groningen
SCP	Sociaal en Cultureel Planbureau
SenterNovem	Agentschap van het ministerie van Economische Zaken, voor duurzaamheid en innovatie
STW	Stichting Toegepaste Wetenschap
Tekes	Fins agentschap voor innovatie
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek
TTI’s	Technologische Topinstituten (zoals NIRM en DPI)
TU/e	Technische Universiteit Eindhoven
TUD	Technische Universiteit Delft
TWA-netwerk	Netwerk van Technisch Wetenschappelijk Attachés van EZ. Verzamelt informatie over technologie en technologiebeleid voor Nederlandse bedrijven, kennisinstellingen, universiteiten en overheid.
UL	Universiteit Leiden
UM	Universiteit Maastricht
UT	Universiteit Twente
UvA	Universiteit van Amsterdam
UvT	Universiteit van Tilburg
VEBON	Vereniging van Beveiligingsondernemers in Nederland; brancheorganisatie
VINNOVA	Zweeds agentschap voor Innovation Systems (www.vinnova.se)
VNG	Vereniging Nederlandse Gemeenten
VU	Vrije Universiteit Amsterdam
VvBO	Verbond van BeveiligingsOndernemingen; koepel van brancheorganisaties
WBSO	Wet Bevordering Speur- en Ontwikkelingswerk; fiscale stimuleringsregeling voor R&D
WEAG	West Euopean Armaments Group, onder meer de WEAG-taxanomy
WUR	Wageningen Universiteit

Ministerie van Economische Zaken

SenterNovem

Colofon

Dit is een publicatie van het
Ministerie van Economische Zaken en
het agentschap SenterNovem.

's-Gravenhage, januari 2008

Extra publicaties kunt u bestellen via www.ez.nl/
publicaties of door te bellen naar 0800-6463951.

Informatie

SenterNovem
Directie Innovatie, taakveld Innovation Intelligence
Postbus 93144
2500 AC Den Haag
Telefoon: 070-3735421
E-mail: innovatieindialoog@senternovem.nl

Publicatienummer: 08O104